pirc

Police Investigations &
Review Commissioner

Data Protection Policy

May 2026

Independent and effective
investigations and reviews

Contents

1. Introduction

The Police Investigations & Review Commissioner (PIRC) is a data controller in terms of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA). As a registered data controller, PIRC has a statutory duty to comply with these provisions. In addition, there are further obligations placed on PIRC by the Data Use and Access Act 2025(DUAA).

The UK GDPR and DPA 2018 introduces legislation which operates in several ways. Firstly, it provides that anyone handling personal information must comply with the data protection principles. Secondly, it provides individuals with rights in relation to information which relates to them and places duties on data controllers to uphold these rights. The DUAA outlines the requirement to have a robust complaints process in place for any concerns raised in relation to data protection issues.

PIRC are required to maintain personal data about individuals for the purpose of satisfying our operational and legal obligations. PIRC recognises 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 PIRC may process include information about current, past and prospective employees; applicants and enquirers; police officers and witnesses; suppliers and other organisations with which PIRC have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the UK GDPR/ DPA. As a named authority within the Scottish Biometrics Commissioner Act 2020, PIRC is obliged to process this type of information in accordance with the Scottish Biometrics Commissioner's code of practice. Therefore, any information of this nature processed in accordance with PIRC's role must be held in accordance with the Records Management Policy.

This policy summarises the key concepts contained in the UK GDPR/DPA DUAA and the responsibilities of PIRC as a data controller.

In addition, the PIRC is a named competent body in the DPA as processing some personal information for Law Enforcement purposes. The additional requirements for compliance for this are incorporated in this policy.

2. UK GDPR Principles and Definitions

PIRC must comply with the seven principles of the UK GDPR which are summarised below. Data must:

1. Be processed fairly and lawfully
2. Be obtained for a specified and legitimate purposes
3. Be adequate, relevant and limited to what is necessary.
4. Be accurate and kept up to date

5. Only be kept for as long as is necessary for the purpose for which it is processed.
6. Personal data must be secure
7. Accountability

PIRC staff who obtain, handle, process, transport and store personal data for us must always adhere to these principles.

Personal data
Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

Controller
Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

Processor
Processors act on behalf of, and only on the instructions of, the relevant controller.

Processing
The term "processing" is very broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data).

Data Subject
An identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Law Enforcement Processing
Processing of personal data by a competent authority for law enforcement purposes. This includes the prevention, investigation, detection or prosecution of criminal offences.

Special Category Data
Special category data is personal data that needs more protection because it is sensitive. Examples of Special Category Data include race, political opinions and health.

Biometric Data
Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images.

3. Types of Data

The UK GDPR lays down conditions for the processing of any personal data and makes a distinction between personal data and "special categories of personal data".

The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person. This definition provides for a wide range of information to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

4. Law Enforcement Processing

As previously mentioned, the PIRC is a named competent body in the DPA and as such is subject to DPA Part 3, Law Enforcement Processing when processing personal data for this purpose.

The seven data protection principles set out in Part 3 differ from the seven data processing principles in the UK GDPR in only one significant way: there is no requirement for personal data to be processed transparently, because of the risk of prejudicing criminal investigations.

Competent authorities and their processors must be able to distinguish between different categories of data subjects, such as suspects, convicts, victims and witnesses.

Data subjects have some of the same rights that they do under the UK GDPR, however the rights to rectification, erasure and restrict processing do not apply to "the processing of relevant personal data in the course of a criminal investigation or criminal proceedings".

Moreover, certain rights under the UK GDPR, as outlined later in section 6 – such as the right to object and the right to data portability – do not exist under Part 3.

5. Handling of Personal/Sensitive Information

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

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

- specify the purpose for which information is used and ensure consent is freely given and recorded
- 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
- protect personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically
- allow only designated users to access software and databases
- wherever possible restrict staff access to printers to secure printing only
- 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, PIRC will ensure that:

- there is a designated Data Protection Officer with specific responsibility for data protection
- all employees understand that they are contractually responsible for following good data protection practice and all employees are appropriately trained to do so
- 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, any disclosure of personal data will be in compliance with approved procedures

6. Individual Rights

Data protection legislation provides individual data subjects with a number of rights.

Right to be Informed

A key transparency requirement of the UK GDPR is for individuals to have the right to be informed about the collection and use of their personal data. Therefore PIRC

will provide individuals with information explaining how PIRC will use any personal information PIRC collect and process, including who PIRC will share this with.

Right of Access – Subject Access Request

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

If any staff receive what appears to be a subject access request, the request should be forwarded in the first instance to the mailbox informationrequests@pirc.gov.scot to be addressed by staff who are responsible for responding to Subject Access Requests. PIRC has one calendar month from the day of receipt to respond to subject access requests under the UK GDPR, so such requests should be forwarded without delay.

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

Right of Rectification

The UK GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete. Requests for rectification must be responded to within one month, whether action is being taken or not, following a request.

Right to Erasure

This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances.

Right to Restricted Processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, PIRC is permitted to store the personal data, but not further process it. In some circumstances the PIRC's statutory obligations will not permit individuals this right, for example when undertaking an investigation at the request of Police Scotland or COPFS.

Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Right to Object

Individuals have the right to object to the processing of their personal data if it is being used for legitimate interests or the performance of a task in the public interest/exercise of official authority. In some circumstances, however, PIRC can

refuse such a request on the basis of legitimate grounds for the processing of personal information and this will be explained to individuals where this applies.

Rights relating to automated decision-making including profiling

Whilst individuals have this right, there are no current circumstances where this is relevant to PIRC.

7. Employee Responsibilities

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

- checking that any personal data that he/she provides is accurate and up to date
- informing of any changes to information previously provided, e.g. change of address
- checking any information that PIRC may send out from time to time, giving details of information that is being kept and processed

Data relating to enquirers/applicants/employees should be reviewed regularly to ensure it is accurate and up to date. All documents, whether handwritten or stored in emails (current or deleted) are potentially disclosable in the event of a subject access request.

8. Data Security

Personal data held by PIRC which relates to others should be kept in accordance with an appropriate level of security, considering 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.

All staff are required to ensure the security of documents or other material / productions when travelling away from the office. Documents relating to investigations must not be left unattended, unless absolutely necessary, and only where this can be stored safely. For example, should it be necessary to leave documents in a hotel room, staff must ensure they are secured in the room safe where available.

It is appreciated that staff may have to take documents with them for the purposes of conducting interviews or undertaking investigations, however as the UK GDPR carries heavy penalties for loss of documents containing personal information, staff should take cognisance of security requirements.

When travelling away overnight, staff must take laptops with them and access documents online, as laptops contain the ability to restrict access via encryption and other security measures such as password protection.

9. Working From Home

Many organisations, including PIRC, allow staff to work from home. Staff must ensure that data protection principles are applied to home working using whatever means possible. As the organisation has progressed to a hybrid model allowing a combination of working between home and office, the need to ensure the security of information remains crucial. Staff can be provided with resources such as lockable cases should they require them to protect the information they hold at home to carry out their duties. In addition, staff are also reminded to take care to restrict access to work information, ensuring that family members are protected in not accessing the information PIRC process, Staff must also not permit others to use the laptop or other equipment provided to them for work purposes, as this could lead to the installation of malware which has the potential to infect the entire network.
In addition this could breach data protection legislation as information must only be viewed by relevant staff.

10. Offences under the UK GDPR

The ICO have powers to administer fines of up to £17.5M depending on the severity of the offence. Offences relating to the breaching of the UK GDPR and DPA by failing to comply with one or more of the principles listed at 2 above. PIRC's Data Breach Notification Procedures are outlined at Appendix A.

11. Publication of Information

Information already in the public domain is exempt from the legislation. This would include, for example, information on employees contained within externally circulated publications, or information published on the PIRC website, such as senior staff backgrounds. Anyone wishing their details to remain confidential in such publications should contact the Head of Corporate Services (HoCS).

12. Subject Consent

Processing personal data relating to a living individual may require us to notify data subjects as appropriate, in most instances.

In some cases, explicit consent is required to process the data which will be recorded. Such processing may be necessary to carry out PIRC's functions and to comply with our statutory obligations.

Contracts of employment provide PIRC with a lawful requirement to process personal data for the purposes of administering and managing 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.

Information about an individual will only be processed 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.

Members of the public requesting a Complaint Handling Review (CHR) from PIRC will be asked to provide their consent in order to allow us to provide the service they require. Whilst applicants have a range of rights outlined earlier, including the right to erasure, in some instances PIRC may continue to retain personal information pertaining to an individual where there are ongoing activities and PIRC require to limit this right to perform our statutory duties.

Activities relating to Investigations PIRC undertake are subject to the UK GDPR, however, any information which relates to processing personal information for the prevention, investigation, detection or prosecution of all criminal offences will be subject to Part 3 of the Data Protection Act 2018, Law Enforcement Processing. In general terms, PIRC will be unable to agree to a request for erasure of personal data made by a data subject due to the purpose for which PIRC is processing their data. In any case, PIRC will inform the individual concerned and explain our legal basis for processing. Depending on the nature of an individual's involvement with a PIRC investigation, PIRC may restrict some of the individual's rights if PIRC consider this will prejudice the investigation.

13. Data Protection Complaints

What is a data protection complaint?

A complaint is an expression of dissatisfaction about the handling of a data subject's personal data or the data of the individual they represent. This can also include dissatisfaction with how PIRC responded to a previous data request, such as those detailed list of rights under section 6.

Making a complaint

The DUAA amends the DPA to include provision for making this type of complaint. It states that controllers must facilitate the making of complaints – this can be done by providing a complaint form that can be completed electronically and by other means.

Data subjects and third parties may make a complaint relating to any aspect of the processing of personal data including individual rights requests.

PIRC will only accept a complaint from a data subject's representative, if the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.
If there is any doubt about the identity of a complainant PIRC will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows:

a. Passport
b. Driving Licence
c. For third parties the identification requirements will vary dependent on their relationship to the data subject. Therefore these will be assessed on a case by case basis.

Investigation and Complaint Outcomes

Once all identification requirements have been met, the investigation will be carried out in line with PIRC's Complaint Handling Procedures (CHP).

The complaint outcome will be communicated to the complainant in writing, normally by email.

If the complainant does not agree with the outcome, they can escalate their complaint to the Information Commissioner's Office (ICO). Information about how to make a complaint to the ICO can be found from the following link:

Making a complaint to the ICO

Complaints can be made using the Complaint Form available from the PIRC website, by email or by post. Completed forms can be emailed using the feedback@pirc.gov.scot email address or by post to the PIRC offices. A blank complaint form is available as Appendix B.

14. Retention and Disposal of Data

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

Information will be kept in accordance with our Records Management Policy Retention Schedule. All staff are responsible for ensuring that information is not kept for longer than necessary. The Information Officer will carry out regular audits to ensure that the retention schedule is being adhered to.

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

15. Registration

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

The UK GDPR 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.

16. Role of the Data Protection Officer

The UK GDPR introduces a duty for organisations to appoint a Data Protection Officer (DPO) if they are a public authority or body, or if they carry out certain types of processing activities. Further details on the role of the DPO can be found on the Information Commissioner Officer's website, of by following this link.

PIRC's Information Officer, is the designated DPO. The DPO has overall responsibility for ensuring compliance with the UK GDPR, for notifying and updating the Information Commissioner (or Scottish Biometrics Commissioner if this involves biometric information) of PIRC's processing of personal data, and for the monitoring and implementation of this policy on behalf of PIRC. The DPO can be contacted by emailing informationrequests@pirc.gov.scot.

17. Review of Policy

This policy indicates how 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 HoCS.

This Policy is a formal PIRC policy and will be reviewed by the PIRC Senior Leadership Team regularly, or at least biannually to ensure compliance with statutory requirements. Any queries regarding this policy, or comments, should be addressed to the employee's line manager.

18. Implementation, Monitoring and Review of this Procedure

The Head of Corporate Services has overall responsibility for implementing and monitoring this procedure, which will be reviewed on a regular basis by the policy owner following its implementation and may be changed from time to time.

Any queries or comments about this procedure should be addressed to the HR@pirc.gov.scot

19. Benchmarks Used in Policy Formulation

- Previous PIRC Policy
- ICO Guidance

Version Control Data

Title:	Data Protection Policy
Author:	Information Officer
Approver:	SLT
Version Number:	V8
Publish Internet/Pulse:	Both
Date of Approval:	April 2026
Summary of last modification:	Addition of DUAA and general update
Modified By:	Information Officer
Next Review Date:	April 2028

APPENDIX A – PIRC Data Breach Notification Procedures

The UK GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioners Office (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

Failing to notify the ICO of a breach, when required to do so, can result in a significant fine of the higher of either £17.5 million or 4% of the undertaking's total worldwide annual turnover in the preceding financial year. The fine can be combined with the ICO's other corrective powers. It is therefore important to make sure there is a robust breach-reporting process in place to ensure PIRC can detect and notify the ICO of a breach, on time; and to provide the necessary details.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, PIRC must also inform those individuals without undue delay.

PIRC are also required keep a record of any personal data breaches, regardless of whether there is a requirement to notify.

Employees are reminded that personal information relating to individuals must not be disclosed to other people, either internally within the PIRC or externally unless PIRC have the written consent of the individual, or PIRC have a legal basis to do so.

What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example:

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

When a personal data breach has occurred, PIRC need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then PIRC must notify the ICO; if it is unlikely then PIRC do not have to report it. However, even in cases which PIRC decide there is no need to report the breach, we still need to be able to justify this decision, and record it on our Breach Register.

Reporting a Breach

All breaches of personal data must be reported to the Information Officer (IO) who is PIRC's designated Data Protection Officer (DPO) under the UK GDPR. In the absence of the IO, the Information Coordinator should be contacted. Under UK GDPR all data breaches of a sufficiently serious nature must be notified to the ICO within 72 hours of us becoming aware of the breach. Therefore there should be no delay in making this notification.

Low Level Breaches

Where the breach is considered to be a low level breach, for example an email sent to the wrong contact in Police Scotland, it is generally determined to be contained within the police IT system and therefore not at risk from unauthorised disclosure to a member of the public. This also applies to emails sent to an incorrect email address within the SCOTS email system. Nevertheless, in both examples, steps must be taken to report this breach internally and provide all necessary evidence, in the format of the email sent in error. The incorrect recipient of the information must also be asked to delete the email from their email account. In some instances, an email response indicating the incorrectly sent email was undeliverable will suffice.

The Breach Register will be updated by the DPO, or Information Coordinator. This will include justification of why the breach does not require to be reported to the ICO, and any correspondence leading to or obtained thereafter will be held on file for the breach.

Serious Breaches

For more serious breaches, PIRC will assess both the severity of the potential or actual impact on individuals as a result of a breach, for example the loss of documentation, the loss of a USB memory stick containing personal information or emails sent to the wrong individual. These cases must be investigated more thoroughly.

The DPO will complete a Breach Report which documents how the breach occurred, what has been done to mitigate the risk and what steps will be taken to prevent a reoccurrence of the breach. The DPO will then notify the ICO and remain the main point of contact. The ICO will want to know the following:

- What happened?
- When it happened?
- How it happened?
- How many people could be affected?
- What sort of data has been breached?
- What did you have in place that could have stopped it?
- What have you done to help the people this affects?
- What have you learned?
- How can you stop similar breaches in the future?

In addition to reporting serious breaches to the ICO, breaches are reported quarterly to the Statutory Advisory Board as it has a role in providing robust scrutiny of the governance processes deployed by PIRC

In the absence of the DPO and Information Co-ordinator, the breach will be recorded by another qualified PIRC Data Protection Practitioner.

The individual(s) affected must also be notified where the breach is sufficiently significant as to be reported to the ICO. The DPO will liaise with management to consider the best way for this to be done.

Further Action

As with any security incident, PIRC will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps. The DPO will agree the next steps with the Head of Service(s) affected. This will vary depending on how the breach occurred and the effect it has had on the individual and the organisation. This may involve changing procedures and/or providing additional training. However in some cases, it may result in disciplinary action.

If information has been deleted in error, early intervention is required to determine if this information can be reinstated from any backup system.

Partner Organisations

In circumstances where PIRC uses another organisation to process personal data on our behalf, for example, payroll and pensions, that other organisation must inform us without undue delay as soon as it is aware of the breach.

This requirement allows us to take steps to address the breach and meet our breach-reporting obligations under the UK GDPR.

Where PIRC use a processor, the requirements on breach reporting must be detailed in the contract between PIRC and the processor.

APPENDIX B – PIRC Data Protection Complaint Form

DATA PROTECTION COMPLAINT

This form should only be used if you have a complaint about how the PIRC has dealt with your personal data.

Are you the data subject whose information is subject to the complaint?	
	Please tick one
YES	
If you are the data subject please supply evidence of your identity, ie original or copy of driving licence, passport, national identity card or photo-pass, and as evidence of address a recent letter or bill from a utility company.	
NO	
Are you acting on behalf of the data subject with their written authority? If so, that authority must be enclosed. Please note that identification as required below must be provided for you and the data subject.	

Details of your complaint

Include the following details where applicable:

- what your complaint is about
- when it happened
- who you dealt with
- how you would like us to resolve the matter.

Be specific about your complaint. Include any reference numbers and dates applicable to your complaint.

Please describe your complaint and specify which personal data protection rule(s) you believe have been infringed.

Please explain what you would like us to do to remedy the alleged violation.

4. When did you become aware of the alleged violation?
Please note that we will not investigate complaints relating to facts that you learned about more than two years ago

If you have supporting documents to substantiate your claim, please state what they are below and how they relate to your complaint. You should then attach copies of those documents with the form.

Contact Details

Data Subject	
Full Name	
Email Address	
Postal Address	
Postal City	
Post Code	
Representative	
Full Name	
Email Address	
Postal Address	
Postal City	
Post Code	

Please save the completed form before printing & posting or emailing it to us together with any attachments.

To send by post to:

Information Governance Team
Hamilton House
Hamilton Business Centre
HAMILTON
ML3 0QA

To send by email to: feedback@pirc.gov.scot

Once PIRC have received your complaint the investigation will be carried out normally within 20 working days. The outcome will be communicated in writing, normally by email.