DATA PROTECTION POLICY

Equality

In accordance with the Equality Act 2010, we make any reasonable adjustment necessary to assist those with a protected characteristic or disability to engage fully with the Commission. Please let us know if you require any assistance with this document.

We are a member of Happy to Translate and can, upon request, provide language assistance with this document or make it available in alternative formats.

0141 270 7030

info@sccrc.org.uk

INTRODUCTION

1.0 Policy statement

1.1 The Scottish Criminal Cases Review Commission (the Commission) recognises the importance of protecting the privacy of its staff and other individuals about whom it obtains, records and discloses information.

1.2 The Commission recognises that the information about those individuals – their 'personal data' – must be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

1.3 The Commission regards the lawful and fair processing of personal data as essential to the successful performance of its statutory functions and its four strategic aims. To that end, the Commission endorses and complies with the principles of data protection.

1.4 The purpose of this policy is to make sure that Board Members and staff, and other stakeholders, are clear about the principles of data protection.

2.0 Policy authorisation

2.1 On 19 September 2025 the Board of the Commission approved this version of this policy.

3.0 Related polices

3.1 This policy must be read in conjunction with the Commission's data retention and disclosure policies, its case handling procedures, its response plan for personal data breaches and its records management plan.

4.0 Definitions

4.1 The terms used in this policy are used in accordance with their interpretation in Article 4 of UK GDPR and Parts 1, 2 and 3 of DPA.

UK GDPR

5.0 Subject matter and scope of UK GDPR

5.1 UK GDPR[1] lays down rules relating to the protection of natural persons with regard to the processing of personal data. It applies to the automated or structured processing of personal data. It applies to the processing of personal data in the context of the activities of a 'controller'[2] or a processor in the UK, regardless of whether the processing takes place in the UK or not.[3]

5.2 The processing of personal data includes collecting, recording, disclosing and destroying such data.

5.3 UK GDPR does not apply to processing of personal data by a competent authority for any of 'the law enforcement purposes' under Part 3 of DPA.[4]

6.0 Data protection principles

6.1 UK GDPR requires that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner
(b) Collected for specified, explicit and legitimate purposes
(c) Adequate, relevant and not excessive
(d) Accurate
(e) Kept no longer than necessary
(f) Processed securely[5]

6.2 The controller shall be responsible for, and be able to demonstrate compliance with, the data protection principles ('accountability').[6]

6.3 A transfer of personal data to third countries or international organisations may be made only if the transfer complies with the conditions for transfer set out in Chapter 5 of UK GDPR.

7.0 Lawfulness of processing

---

1 In force on 1 January 2021.
2 The Board of the Commission is the controller in relation to the personal data that the Commission processes.
3 Articles 1–3 of UK GDPR.
4 Article 2 of UK GDPR.
5 Article 5 of UK GDPR.
6 Article 5 of UK GDPR.

7.1 UK GDPR provides that processing shall be lawful only if at least one of the conditions listed in Article 6(1) or (where relevant) Article 9(2) applies.

7.2 Where it is processing personal data under UK GDPR, the Commission is generally doing so either for the performance of a contract or for the performance of public task[7] (see the Commission's privacy notices), but it may do so also with consent, for compliance with a legal obligation to which it is subject, to protect the vital interests of an individual or for the purposes of a legitimate interest pursued by the Commission.[8]

7.3 The Commission processes special categories of personal data under Article 9 of UK GDPR (see below and the Commission's privacy notices).

7.4 Different rules apply where the Commission is processing personal data for a law enforcement purpose under Part 3 of DPA (see below: '**Law enforcement processing**').

8.0 Consent

8.1 The Commission does not, generally, process personal data on the basis of consent. Where it does, the Commission will demonstrate that the individual has consented to the processing of his or her personal data.[9]

8.2 An individual who has provided their consent has the right to withdraw it at any time.

9.0 Rights of individuals

9.1 UK GDPR provides for certain rights of individuals, including the following:

(1) To be informed
(2) Access
(3) Rectification
(4) Erasure
(5) Restriction
(6) To object[10] (see the Commission's privacy notices)

10.0 Restrictions

10.1 The Secretary of State may restrict the scope of the obligations and rights under Articles 12–22 of UK GDPR.[11]

11.0 Responsibilities

11.1 It is, ultimately, the responsibility of the controller – the Board of the Commission – to implement appropriate technical and organisational measures to make sure, and to be able to demonstrate, that processing is carried out in accordance with UK GDPR.[12]

---

7 Article 6(1)(b) and (e) of UK GDPR.
8 Article 6(1)(a), (c) (d) and (f) of UK GDPR.
9 Article 7 of UK GDPR.
10 Articles 12–22 of UK GDPR.
11 Article 23 of UK GDPR.
12 Article 24 of UK GDPR.

11.2 It is, however, the Commission's designated 'data protection officer' (DPO) who takes day-to-day responsibility for data protection compliance.[13] The Commission designated DPO is Stephen Lynn (contact: info@sccrc.org.uk). The DPO:

- Informs and advises the Commission and its staff about their obligations to comply with UK GDPR (and DPA)
- Monitors compliance with UK GDPR (and DPA), including managing internal data protection activities and advising on data protection impact assessments
- Trains staff and conducts internal audits
- Is a point of contact for the 'data subject'[14] and the Information Commissioner's Office (ICO)
- Reports to the Board of the Commission[15]

TYPES OF PROCESSING

12.0 Types of processing

12.1 The processing that the Commission carries out falls into two broad types:

- **General processing**: including the processing of personal data about Board Members, staff, former staff and prospective staff ('Board Members/staff').
- **Law enforcement processing**: the processing of personal data so that the Commission can carry out its primary statutory function,[16] including the processing of data about applicants, witnesses in cases that the Commission is reviewing or has reviewed, and other individuals whose data feature in the cases that the Commission is reviewing or has reviewed.

13.0 General processing

Purposes

13.1 The Commission processes personal data for, among other purposes, the following specified purposes:

- Recruitment
- Equal opportunities monitoring
- Administering maternity, paternity, dependant-care and other leave
- Disciplinary and grievance procedures

---

[13] Article 37 of UK GDPR.
[14] The individual to whom the data relates.
[15] Articles 38 and 39 of UK GDPR.
[16] Which is that the Commission may, on the consideration of any conviction of a person in Scotland or the sentence imposed in such a case, refer the case to the High Court of Justiciary for determination where it believes there may have been a miscarriage of justice and it is in the interests of justice to make such a reference: s194B and C of the Criminal Procedure (S) Act 1995 (CPSA).

- Payroll
- Holidays and absences
- The proper administration of the contract of employment
- On premises CCTV and video controlled entrance
- Procurement
- Property, financial and corporate
- Where individuals contact the Commission seeking information

Rights of access, rectification, erasure etc. (see the Commission's privacy notices)

13.2 Individuals have the right to gain access to data that the Commission holds about them. The right applies, for example, to information held in sickness records, disciplinary, grievance or training records, appraisal or performance-review notes, emails, general personnel files and interview notes.

13.3 As soon as reasonably practicable, but within one month of his receipt of the written request for access to the personal data, the DPO or the Commission's Director of Corporate Services (DOCS) will provide the requester with his or her personal data, in an intelligible form (including, where appropriate, by electronic means), and the following information:

- The purposes of the processing
- The categories of personal data
- The recipients to whom the personal data have been disclosed (if any)
- The right to request the Commission to rectify, erase and restrict the processing of personal data or restriction, and the right to object to such processing
- The right to lodge a complaint with the ICO
- (Where the personal data have not been collected from the data subject) any available information about their source[17]

13.4 The Commission will not disclose personal data where it adversely affects the rights and freedoms of others.[18]

13.5 Individuals have the right to obtain from the Commission, without undue delay, the following: the rectification of inaccurate data about them; the erasure of their personal data where, for example, those data are no longer necessary in relation to the purposes for which they were collected and otherwise processed; and the restriction of processing of their personal data. The DPO or the DOCS will, where it is applicable to do so, rectify, erase and restrict the data, and notify the data subject (see the Commission's privacy notices).[19] These rights are subject to the restrictions contained in Schedules 2 and 3 to DPA. Where the Commission restricts access to a data subject's personal data it will inform them of this in writing.

Excluded information

[17] Article 15(1) of UK GDPR.
[18] Article 15(4) of UK GDPR.
[19] Articles 16–19 of UK GDPR.

13.6 Staff are not entitled to have access to certain information, including the following information:

- Confidential references about the individual concerned given on behalf of the Commission by, for example, one of its Board Members or its Chief Executive
- Any documents privileged on the grounds of legal professional privilege
- Data used for the prevention or detection of a crime
- Personal data being processed for the purposes of management forecasting or planning

13.7 References received from other people are not treated in the same way as references about a staff member that a Board Member or the Chief Executive has given.

13.8 In the former case, and where the individual to whom the reference relates asks the Commission to disclose to him or her the information in the reference, the Commission will ask the referee whether he or she consents to the disclosure of the information to the individual. Where the referee states that he or she does not want the Commission to disclose the reference, the Commission will provide the reference to the individual only if it considers that it is reasonable in all the circumstances to comply with the request without the referee's consent. In taking such a decision, the Commission will take into account the following factors:

- Any express assurance of confidentiality given to the referee
- Any relevant reasons the referee gave for withholding the information
- The potential or actual effect of the reference on the individual
- The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- That good employment practice suggests that an employee should have already been informed of any weakness that he or she has.
- Any risk to the referee
- Whether it is possible to keep the identity of the referee confidential

Accuracy

13.9 The Commission makes sure that, so far as possible, personal data that it keeps are accurate.

13.10 Board Members and staff are required to inform the DOCS of changes in their contact details as soon as reasonably practicable, in order to assist the Commission in keeping their personal data up to date.

Security[20]

[20] Discussed in more detail in para 14.16 below, in terms of '**Law enforcement processing**'.

13.11 Personal data are kept in a secure filing cabinet or on a password-protected computer file. We make sure that, as far as possible, paper-based data are stored in organised and secure systems. Only those staff who have a legitimate business need to access such data may access them.

13.12 Personal data about former staff is separated from personal data about existing staff, and is placed in marked folders. Each folder is marked with the name of the former staff member, his or her date of birth and the dates of employment.

13.13 The Commission operates a clear desk policy at all times in respect of personal data.

Retention

13.14 The Commission keeps personal data in accordance with its data retention policy.

13.15 All documents containing personal data that are destroyed are destroyed securely and in accordance with the data protection principles. The DOCS is responsible for overseeing the destruction of personal data.

Post

13.16 All confidential post must be opened by the addressee only.

Use of photographs

13.17 The Commission seeks consent from a Board Member or a staff member before displaying a photograph in which he or she appears. It will remove any photograph where the Board Member or staff member asks it to do so.

Contact details

13.18 The contact details of a Board Member or staff member are made available only to other Board Members or other staff members. They are not passed on to anyone outside the Commission without the consent of the Board Member or the staff member (unless the Commission is entitled by law to do so).

13.19 Any other employee-related information is not accessed during the day-to-day running of the organisation.

13.20 The emergency contact details of each Board Member and each staff member are kept in an appropriate file to be used in emergency situations.

Third-party disclosure requests

13.21 The Commission may receive requests from a third party for information about Board Members/staff. In dealing with such requests, the Commission has a responsibility to safeguard the interests of the Board Members/staff.

13.22 In some cases the Commission will have no choice but to respond positively to such a request – where, for example, the police need information in connection with a criminal investigation. In other cases a third party may want information in connection with a legal action. The Commission may disclose the information in such cases where it is entitled by law to do so.

13.23 The Board of the Commission takes any decision about whether to comply with such a request.

Special categories of personal data

13.24 The special categories of personal data are:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
- Genetic data or biometric data
- Health data
- Data about an individual's sex life or sexual orientation[21]

13.25 Article 9(1) of UK GDPR prohibits the processing of special categories of personal data unless a condition in Article 9(2) (and a condition in Schedule 1 to DPA) is met. Article 10 of the UK GDPR limits the processing of personal data relating to criminal convictions and offences, permitting it only under the control of official authority or where the processing is authorised by domestic law subject to conditions listed in Parts 1, 2 or 3 of Schedule 1 to DPA. Where the Commission is processing criminal conviction data it will, generally, be processing this for the purposes of law enforcement under DPA (see below).

13.26 This policy document is a requirement under Part 4 of Schedule 1 to DPA.

13.27 The Commission's privacy notices set out its legal bases for processing the personal data held under Articles 9 and 10 and processed in terms of a condition under Schedule 1 to DPA.

13.28 How the Commission meets the six data protection principles (as listed above) in relation to the processing of special categories of personal data:

Lawful, fair and transparent

- Our Privacy Notices are on our website: - www.sccrc.org.uk.

- Where explicit consent is requested from an individual, we shall provide the individual with details about what special category of personal data is involved, what will happen to his or her personal data and the length of time we shall keep the data, as well as telling the individual about the right to withdraw his or her consent at any time.

Specified, explicit and legitimate purposes

- Processing is restricted only to that which is necessary for the relevant purpose and the data will not be used for a purpose which is incompatible with the relevant purpose.

- If we intend to carry out further processing (and that processing is not based on explicit consent), and the purpose does not fall within Schedule 2 of DPA, we shall determine whether the proposed processing is compatible, in terms of Article 6(4) of UK GDPR. And we shall, prior to the proposed processing, provide the individual with information about that other purpose and with any relevant information, in terms of Article 13(3) and Article 14(4) of UK GDPR.

[21] Article 9(1) of UK GDPR.

Adequate, relevant and not excessive

- Processing is restricted only to that which is necessary for the relevant purpose. Our data protection training emphasises this.

Accurate

- We shall make sure that, as far as possible, special category of personal data that we process is accurate and up to date. Where such data are found to be inaccurate, we shall rectify or erase the data.

Kept no longer than necessary

- We keep special category of personal data in accordance with our data retention policy.
- Where an individual withdraws his or her consent to the processing of special category of personal data (and where we are processing such data on the basis of consent), we shall destroy the data on receipt of the withdrawal-of-consent notice unless there is an overriding purpose for continued processing.

Securely

- We have implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data that we are processing: see paragraph 14.6 below.
- All Members and staff undertake data protection training; all staff undertake training in our case management system.

Absence records

13.28 The term 'absence record' (as opposed to sickness and injury records[22]) is used to describe a record that may give the reason for absence as 'sickness' or 'accident', but does not include any reference to specific medical conditions. It does not constitute data concerning health.

13.29 The Commission restricts its record-keeping in this area of processing, so far as practicable, to absence records.

14.0 Law enforcement processing

14.1 Part 3 of DPA, which implements the Law Enforcement Directive,[23] provides for the processing of personal data by competent authorities for 'the law enforcement purposes'.

[22] Sickness and injury records include information about the physical and mental health of employees. They constitute 'data concerning health', as defined in Article 4(15) of UK GDPR and processed in accordance with Article 9 of UK GDPR.

[23] Which means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

14.2 The law enforcement purposes are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[24]

14.3 Processing of personal data for a law enforcement purpose must comply with the data protection principles set out in ss34–40 of DPA.[25] In particular, processing of personal data for such a purpose must be, in terms of 'the first data protection principle', 'lawful and fair'.[26]

14.4 Where the data subject has not consented to the processing, the processing of data for any of the law enforcement purposes is lawful only if, in terms of the first data protection principle, the processing is necessary for the performance of a task carried out for that purpose by a competent authority within the meaning of s30 of DPA.[27]

14.5 The Commission is a competent authority within the meaning of s30 of DPA (it is listed as such in Schedule 7 to DPA). It is a 'controller'[28] for processing of data for the law enforcement purposes.

Purpose

14.6 The Commission's legal basis for processing personal data for a law enforcement purpose derives from its functions and powers as set out in s194A–T of CPSA. In other words, the Commission processes such data so that it can carry out its primary statutory function (as noted above).

14.7 Such data include the data of the applicants whose cases that the Commission is reviewing or has reviewed. They may also include the data of witnesses in those cases and of other individuals. They are collected, recorded and – in limited circumstances – disclosed to third parties.

The controller's general duties and the data subject's rights of access, rectification, erasure etc.

14.8 The controller's general duties and the data subject's rights of access, rectification, erasure etc. where data is processed for law enforcement purposes are set out in ss44–48 of DPA. The Commission makes the information set out in s44(1)and (2) of DPA available in this policy document, in its Privacy Notices and in its Data Retention Policy.

14.9 The Commission may, having regard to the fundamental rights and legitimate interest of the data subject, restrict the data subjects right of access under s45(1) where it considers it necessary and proportionate to do so in line with one of the conditions listed at s45(4). In such circumstances the Commission will inform the data subject of this and the reasons for restriction as well as the information at s45(5)(a)-(c).

14.10 Sections 44-48 do not apply in relation to the processing of 'relevant personal data'[29] in the course of criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal penalty.[30] Where it is processing personal data for a law enforcement

[24] Section 31 of DPA.
[25] Those principles mirror the principles set out in Article 5 of UK GDPR.
[26] Section 35(1) of DPA.
[27] Section 35(2)(b) of DPA.
[28] In terms of s32 of DPA.
[29] As defined in s43(4) of DPA.
[30] Section 43(3) and (4) of DPA.

purpose, the Commission is processing an applicant's personal data which may include relevant personal data.

14.11 The Commission take appropriate measures to protect the data subject's rights and freedoms and legitimate interests.

Disclosure

14.12 It is only Board Members and staff who will normally have access to personal data. All Board Members and staff are made aware of this policy and their obligation not to disclose such data to anyone who is not supposed to have them.

14.13 Personal data is passed to a person outside the Commission without the data subject's consent only where the Commission is entitled by law to do so. The Commission may disclose such data to:

- Applicants to the Commission
- Legal representatives of the applicant
- Scottish Court and Tribunal Service
- The Crown Office and Procurator Fiscal Service
- Police Scotland
- Expert witnesses[31]

Accuracy and relevancy

14.14 The Commission takes reasonable steps to make sure that it stores and retains only those personal data which are or were relevant to its case reviews.[32]

14.15 It will make sure that, as far as possible, personal data it keeps are accurate.[33]

Security

14.16 The Commission handles all personal data it processes in a secure and responsible manner.[34] Its security arrangements – both in terms of its physical and technological security and its management and organisational security – reflect the large volumes of personal data it processes and the levels of sensitivity and confidentiality of those data, and the harm that might result from the improper use of personal data or from their accidental loss or destruction. A summary of those arrangements follows.

- The Commission classifies most of the personal data that it processes as 'official'.[35]

- The personal data the Commission processes are subject to extensive physical security arrangements: the Commission's premises are protected by an alarm, a shutter, security lighting and CCTV; visitors to its premises are subject to controlled access.

---

31 See the Commission's disclosure policy.
32 Section 37 of DPA.
33 Section 38 of DPA.
34 Section 40 of DPA (see also Article 32 of UK GDPR).
35 May-2018_Government-Security-Classifications-2.pdf (publishing.service.gov.uk)

- The Commission operates its own IT system from its premises, which has been designed with specific security arrangements, which are subject to ongoing testing. For example, the personal data kept electronically are kept on a password-protected computer file; the IT system has been installed with a firewall, an anti-spyware tool and virus-checking software, and downloads the latest security updates; regular back-ups of all data on its computers are taken; and all such data are securely removed from its old computers before the computers are disposed.

- Physical information the Commission sends and receives is undertaken in a secure manner, using vetted courier services or the Royal Mail.

- Where it sends personal data electronically, the Commission does so using a secure email system such as Egress Switch or the Criminal Justice Secure Mail system.

- The Commission makes sure that, as far as possible, the personal data kept in a paper-based system are kept in an organised and secure system.

- The Commission has put in place procedures that staff must follow concerning, among other things, the instruction of a third party and personal data given to the third party, personal data that staff take out the office, and the use of letters and emails (see the Commission's case handling procedures).

- All personal data kept off-site are kept securely. Where, for example, Board Members and staff are working from home, the data is held electronically, in a password-protected and encrypted laptop or iPad.

- All staff are subject to Disclosure Scotland 'standard disclosure'; 'enhanced disclosure' is in place for Board Members and all staff at legal officer level and above; Board Members and several key staff have been cleared to 'security clearance' level.

- All waste paper containing personal data is destroyed securely.

- The Commission operates a clear desk policy at all times in relation to personal data.

Retention

14.17 The Commission retains all personal data in accordance with s39 of DPA: see its data retention policy.

14.18 All documents containing personal data are destroyed securely and in accordance with the data protection principles. The DPO is responsible for overseeing the destruction of such data.

Sensitive processing for the law enforcement purposes

14.19 'Sensitive processing' means the processing of:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
- Genetic data or biometric data
- Health data

- Data about one's sex life or sexual orientation[36]

14.20 Sensitive processing for the law enforcement purposes is permitted in either of the following two situations:[37]

- The individual has given consent to the processing for the specific purpose; or
- Processing is strictly necessary for the law enforcement purposes and meets at least one of the conditions in Schedule 8 to DPA.[38]

14.21 In either situation the controller must have an appropriate policy document (APD) in place.[39] This policy document is the Commission's APD.

14.22 How the Commission meets the six data protection principles set out in ss34–40 of DPA in relation to sensitive processing for the law enforcement purposes:

Lawful, fair and transparent

- Processing is strictly necessary for the law enforcement purposes and meets at least one of the conditions in Schedule 8 to DPA, in that it is necessary for the exercise of a function conferred on us by an enactment or rule of law (by virtue of s194A–T of CPSA), and for reasons of substantial public interest (condition 1).
- Alternatively, in terms of Schedule 8, processing for the law enforcement purposes is, on occasion, necessary for the administration of justice (condition 2), for protecting an individual's vital interests (condition 3), for safeguarding of children or individuals at risk (condition 4), or in relation to legal claims (condition 6).

Specified, explicit and legitimate purposes

- Sensitive processing is restricted only to that which is necessary for the law enforcement purposes and the data will not be used for a purpose which is not a law enforcement purpose unless that use is authorised by law.

Adequate, relevant and not excessive

- Personal data collected for the law enforcement purposes are restricted only to those which are necessary for the relevant purpose. Our data protection training emphasises this.

Accurate

- We shall make sure that, as far as possible, personal data we process are accurate and up to date. Where such data are found to be inaccurate, we shall rectify or erase the data.

Kept no longer than necessary

36 Sections 35(8) of DPA.
37 Section 35(3) of DPA.
38 Section 35(4) and (5) of DPA.
39 Section 35(4)(b) and (5)(c) and s42 of DPA.

- We keep personal data in accordance with our data retention policy.

Securely

- We have implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data that we are processing: see paragraph 14.6 above.

- All Members and staff undertake mandatory data protection training; all staff undertake training in our case management system.

14.23 Where it carries out sensitive processing for a law enforcement purpose, the Commission does so in accordance with the safeguarding requirements set out in s42 of DPA.

OTHER MATTERS

15.0 Personal data breaches

15.1 A 'personal data breach' means a breach of security leading to the destruction, loss, alteration and unauthorised disclosure of, or access to, personal data.

15.2 The Commission recognises that, if a personal data breach occurs, it is important to deal with the breach effectively, in accordance with the requirements set out in Articles 33 and 34 of UK GDPR.

15.3 Accordingly, the Commission has a 'response plan for personal data breaches'. The plan sets out the Commission's strategy for dealing with a breach of security, and includes the following three elements:

- Containment and recovery
- Notification of the breach
- Evaluation and response

15.4 Where a personal data breach is likely to result in a 'risk' to the rights and freedoms of individuals – i.e., such a breach, if unaddressed, is likely to have a significant detrimental effect on individuals, resulting in discrimination, damage to reputation, financial loss or loss of confidentiality – the Commission will report the breach to the ICO without undue delay, and not later than 72 hours after it became aware of the breach.[40] In doing so, it will:

- Record the breach
- Describe the nature of the personal data breach
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- Communicate the name and contact details of the DPO
- Describe the likely consequences of the breach
- Describe the measures it has taken, or proposes to take, to address the breach[41]

[40] Article 33(1) of UK GDPR.
[41] Article 33(3) of UK GDPR.

15.5 Where the personal data breach is likely to result in a 'high risk'[42] to the rights and freedoms of individuals, the Commission will inform those individuals concerned directly and without undue delay.[43]

15.6 Where it decides to tell individuals about a breach, the Commission will provide the name and contact details of the DPO and will describe, in clear and plain language, the nature of the breach, the likely consequences of the breach and the measures it has taken, or proposes to take, to address the breach.

The law enforcement purposes

15.7 Where it is processing personal data for a law enforcement purpose, in terms of Part 3 of DPA, and there is a data breach, the Commission will apply the relevant DPA provisions about notification to the ICO and the data subjects, namely ss67 and 68 of DPA, the terms of which mirror the above-mentioned steps about notification.

16.0 Data Protection Impact Assessment (DPIA)

16.1 A DPIA is a tool that can help an organisation identify the most effective way to comply with its data protection obligations and to meet individuals' expectations of privacy.

16.2 The Commission will carry out a DPIA when:

- It is using new technologies, or using technologies in a new environment; and
- The processing of personal data is likely to result in a high risk to the rights and freedoms of individuals[44] (which will include large scale processing of special categories of data).

17.0 Data sharing

17.1 Where it shares data with stakeholder organisations, the Commission will adhere to the ICO's Data Sharing Code of Practice: see here.

18.0 Offences

18.1 It is an offence for a Board Member or a staff member, knowingly or recklessly and without the Commission's consent, to obtain or disclose personal data, or to procure the disclosure of the personal data, to another person outwith the Commission.[45]

18.2 It is an offence for a Board Member or a staff member to sell, or to offer to sell, personal data which have been unlawfully obtained.[46]

19.0 Compliance

19.1 It is the responsibility of all Board Members and all staff to make sure that they are familiar with the terms of this policy and that they comply with it at all times.

---

[42] A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.
[43] Article 34 of UK GDPR.
[44] Articles 35 and 36 of UK GDPR.
[45] Section 170(1) of DPA.
[46] Section 170(4) of DPA.

19.2 The DPO will carry out periodic checks to ascertain whether staff are complying with procedures concerning data protection and records management matters.

19.3 Any questions or concerns about the application of this policy should be referred to the DPO.

20.0 Review

20.1 The DPO will review this policy at least annually.

Date first approved	16 August 2013
Date of this review	24 May 2024
Date of next review	September 2026