DATA PROTECTION POLICY

1.0 Policy statement

1.1 The Scottish Criminal Cases Review Commission ("the Commission") recognises the importance of protecting the privacy of all employees and other individuals about whom it obtains and stores information. The Commission recognises that such information, or personal data, must be dealt with properly and securely, however it is collected, recorded and used – whether on paper, electronically or recorded on other material – in accordance with the statutory framework of rights and duties designed to safeguard personal data, as set out in the Data Protection Act 1998 (DPA).

1.2 The Commission regards the lawful treatment of personal data as being crucial to the successful and efficient performance of its statutory functions and its four corporate objectives, and to the maintenance of confidence between those individuals and organisations with whom it deals. To that end, the Commission fully endorses and adheres to the principles of data protection.

1.3 The Commission recognises that any failure by it to adhere to DPA is unlawful and could result in the taking of legal action against the Commission, individual Board Members or individual employees.

2.1 Purpose

2.1 The purpose of this policy is to ensure that Board Members, employees and the Commission's other stakeholders are clear about the purpose and the principles of data protection, and to ensure that the Commission has procedures in place which are consistently followed.

3.0 Policy authorisation

3.1 The Board of the Commission approved this policy on 16 August 2013.

4.0 Related polices

4.1 This policy must be read in conjunction with the Commission's data retention policy, its disclosure policy, its case handling procedures and its records management plan.[1]

5.0 Definitions

5.1 The terms from DPA used in this policy are defined in the attached glossary of terms (see appendix 1 of this policy), and are used in accordance with their usage in DPA and by the Information Commissioner's Office (ICO).

6.0 Principles

6.1 DPA regulates the processing of data relating to living and identifiable individuals; the individual who is the subject of the personal data is called the "data subject". Processing includes the obtaining, holding, using or disclosing of such data. There are eight straightforward principles which underpin DPA. In summary, they require that the data must be:

1. **processed fairly and lawfully, and the processing must meet one of the conditions in Schedule 2 to DPA (and in the case of sensitive personal data, it meets also one of the conditions in Schedule 3);**
2. **processed for specified purposes;**
3. **adequate, relevant and not excessive;**
4. **accurate;**
5. **not kept longer than necessary;**
6. **processed in accordance with the data subject's rights;**
7. **secure; and**
8. **not transferred to a country outside the European Economic Area, without adequate protection.**

6.2 The principles apply to personal data which are held on the Commission's computer systems or in its manual filing systems from which the data subjects are identifiable ("relevant filing systems").

7.0 Responsibilities

7.1 For the purposes of DPA, the Commission is a "data controller". As such, the Board of the Commission is, ultimately, responsible for ensuring the security of all personal data the Commission holds about Board Members, employees, applicants (to the Commission) or any other individuals. However, it is the responsibility of the Commission's Head of Casework (HOC) and its Director of Corporate Services (DOCS) to put in place the relevant procedures to ensure that data are processed in accordance with the eight data protection principles.

7.2 Notwithstanding the above, it is the responsibility of all Board Members and all Commission employees to ensure that they are familiar with the terms of this policy and that they comply with it at all times.

[1] The Commission's records management plan, as required by the Public Records (Scotland) Act 2011, was agreed on 30 April 2014 by the Keeper of the Records of Scotland.

7.3 It is the responsibility of the HOC to ensure that the Commission is registered annually with the register of data controllers held by the ICO, and to ensure that the Commission's register entry report is accurate.

8.0 Procedures

8.1 The Commission has developed the under-noted procedures to ensure that it meets its responsibilities under DPA. In doing so, the Commission has categorised the personal data it processes into the following two broad categories:

- **Non-case-related data**: data about Board Members, employees, former employees and prospective employees

- **Case-related data**: data about applicants, witnesses in cases the Commission is reviewing or has reviewed, and any other individuals whose data feature in the cases the Commission is reviewing or has reviewed

9.0 Non-case-related data

Purposes

9.1 The Commission processes personal data about Board Members, employees, former employees and prospective employees. Such data are processed for, among other purposes, the following specified purposes:

- Recruitment
- Equal opportunities monitoring
- Administering maternity, paternity, dependant-care and other leave
- Disciplinary and grievance
- Payroll
- Holidays and absences
- The proper administration of the contract of employment

Contact details

9.2 The contact details of a particular Board Member or employee are made available only to other Board Members or other employees. They are not passed on to anyone outside the Commission without the explicit consent of the Board Member or the employee concerned (unless the Commission is obliged by law to do so). Any other employee-related information is not accessed during the day-to-day running of the organisation.

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

Access

9.4 Board Members and employees of the Commission, like any other individuals, have the right to gain access to data the Commission holds about them. The right

is known as "subject access". It applies, for example, to sickness records, disciplinary, grievance or training records, appraisal or performance review notes, emails and information held in general personnel files, and interview notes, whether or not those data are held as computerised files or as structured paper records.

9.5 Each Board Member and each employee will be supplied with a copy of his or her personal data the Commission holds about him or her if he or she makes a subject access request in writing to the DOCS. Within 40 calendar days of his receipt of the request, the DOCS will respond in the following way:

- Give a description of the type of data the Commission keeps about him or her, the purposes for which it is used and the types of organisations on to which it may be passed (if any).

- Provide his or her personal data in an intelligible form.

- Tell him or her about the source of the information constituting the personal data.

9.6 Where compliance with such a request for data would result in the disclosure of information about another individual, the Commission need not comply with the request unless the other individual – the third party – consents to its disclosure, or it is reasonable in all of the circumstances to disclose the information about the third party without such consent.

9.7 Employees 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 the 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.

9.8 References received from people or organisations are not treated in the same way as references about an employee of the Commission given by a Board Member or the Chief Executive. In the former case, if the individual about whom the reference was made 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. If the referee states that he or she does not want the Commission to release 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 he or she has.

- Any risk to the referee.

- Whether it is possible to keep the identity of the referee secret.

Third-party disclosure requests

9.9 The Commission may receive requests from a third party for information about Board Members or employees. In dealing with such requests, the Commission has a responsibility to safeguard the interests of the Board Members and the employees. In some cases, however, the Commission will have no choice but to respond positively to such a request for information – where, for example, the police want information in connection with a criminal investigation. In other cases, a third party may want information to pursue legal action. The Commission may choose to disclose the information in such cases if the conditions of a relevant exemption allowing for the disclosure of information apply.

9.10 The Board of the Commission takes any decisions about whether to comply with third-party disclosure requests.

Sickness and injury records/absence records

9.11 Sickness and injury records include information about the physical and mental health of employees. They constitute "sensitive personal data". The term "absence record" 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 sensitive personal data. The Commission restricts its record-keeping in this regard, so far as practicable, to absence records.

Post

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

Accuracy

9.13 The Commission will take reasonable steps to ensure that the case-related data it keeps are accurate.

9.14 Board Members and employees 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.

9.15 If a Board Member or an employee believes that any information contained within personal data relating to him or her is inaccurate, he or she is entitled to make a written request to the DOCS to have his or her personal data corrected.

Security

9.16 The data are kept in a secure filing cabinet or on a password-protected computer file (see also **10.8**). Every effort is made to ensure that paper-based data are stored in organised and secure systems. Only those employees who have a legitimate business-need to access such personal data may access them.

9.17 Personal data about former employees will be separated from personal data about existing employees, and will be placed in a clearly marked folder. The folder will be marked with the name of the former employee, his or her date of birth and the dates of employment.

9.18 The Commission operates a clear desk policy at all times in respect of non-case-related data.

Use of photographs

9.19 The Commission will, so far as is practicable, seek consent from Board Members and employees before displaying photographs in which they appear. If that is not possible, it will remove any photograph where a Board member or an employee asks it to do so.

Retention of data

9.20 The Commission keeps such data in accordance with its data retention policy and with its associated data retention and destruction procedures.

9.21 All documents containing such data that are destroyed are destroyed securely and in accordance with the data protection principles. The DOCS has responsibility for overseeing the destruction of such data.

10.0 Case-related data

Purposes

10.1 The Commission has to ingather information about the cases it reviews. Such case-related data enable the Commission to carry out its primary function: namely, the Commission, on the consideration of any conviction of a person in Scotland, or of a sentence imposed in respect of such a conviction, may, if it thinks fit, refer the case to the High Court for determination. Case-related data contain the personal data and sensitive personal data of the applicants whose cases the Commission is reviewing or has reviewed. They may also contain the personal data and sensitive personal data of witnesses in those cases and of other individuals. The data are obtained, stored and – in limited circumstances – disclosed to third parties to enable the Commission to perform its primary function.

Consent

10.2 The Commission obtains the explicit consent of each applicant for it to obtain, to record and to hold information about his or her case, and for it to disclose information about his or her case in accordance with its duties laid down by law (see the Commission's application form, "Part 9: Data Protection").

Access

10.3 It is only Board Members and employees who will normally have access to case-related data. All Board Members and employees are made aware of this policy and their obligation not to disclose case-related data to anyone who is not supposed to have them.

10.4 Case-related data will not be passed to anyone outside the Commission without the data subject's explicit consent, unless specific exemptions in DPA allow for the disclosure of information where there would otherwise be a breach of DPA. For example, the disclosure of the information is required by law, or is necessary for the purpose of, or in connection with, any legal proceedings. This would include data the Commission discloses to a third-party expert it has instructed in a case review.

10.5 An individual will be supplied with a copy of any of his or her personal data the Commission holds about him or her if he or she makes a subject access request to the Commission, unless a specific exemption allows the Commission to withhold the data.

10.6 All requests for information must be passed, in the first instance, to the Commission's information officer.

Accuracy

10.7 The Commission takes reasonable steps to ensure that the case-related data it keeps are accurate.

Security

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

- The data the Commission processes are subject to extensive physical security arrangements; the Commission classifies most of the data it processes as "official".[2]

- The Commission's premises are protected by an alarm, a shutter, security lighting and CCTV; visitors to its premises are subject to controlled access.

- The Commission operates its own IT system from its premises, which has been designed with specific security arrangements, arrangements which are subject to ongoing testing. For example, the 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 the Commission sends case-related data electronically to its key stakeholder organisations in the justice sector, it does so using a secure form. For example, it exchanges case-related data electronically with some of its key stakeholders in the justice sector by means of the Criminal Justice Secure eMail Service.

- The Commission makes every effort to ensure that case-related data kept in a paper-based system are kept in organised and secure systems.

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

- All case-related data kept off-site are kept securely.

[2] See the Government Security Classifications, as issued by the Cabinet Office, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

- All Board Members and employees are subject to at least Disclosure Scotland Standard Disclosure; Enhanced Disclosure is in place for all staff at legal officer level and above; several key employees have been cleared to SC level.

- All waste paper containing case-related data is destroyed securely.

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

10.9 In addition, the Commission is always looking to strengthen its procedures concerning the sending and receiving of data. To that end, it now uses the "Diligent Boardbooks" system, which enables the electronic exchange of case-related data between Board Members and employees to be done securely, and which obviates the need for the Commission to send such data in hard copy to Board Members.

Retention of data

10.10 The Commission retains all case-related data in accordance with its data retention policy and with its associated data retention and destruction procedures.

10.11 All documents containing case-related data that are destroyed are destroyed securely and in accordance with the data protection principles. The HOC has responsibility for overseeing the destruction of such data.

11.0 Breaches of security

11.1 The Commission recognises, however, that, if, despite the security measures it has put in place to protect the personal data it holds, a breach of security occurs, it is important to deal with the breach effectively. Accordingly, the Commission has a "breach-management plan". The plan sets out the Commission's strategy for dealing with a breach of security, and includes the following four elements:

- Containment and recovery
- Assessment of ongoing risk
- Notification of the breach
- Evaluation and response

11.2 The Commission will report to the ICO any "serious" breaches of its security which resulted in the loss, release or corruption of personal data. In considering whether any breach should be reported to the ICO, the Commission will have regard to the potential detriment to data subjects, the volume of personal data lost, released or corrupted, and the sensitivity of personal data lost, released or corrupted.

12.0 Information-sharing protocols

12.1 The Commission recognises the value of facilitating information-sharing. It has established information-sharing protocols or agreements (ISPs) with certain stakeholder organisations in the justice sector, the purpose of which is to facilitate

the provision of information from those organisations to the Commission, thus assisting the Commission in fulfilling its statutory functions. Those ISPs comply with DPA, and have regard to the Data-sharing Framework issued by the ICO. The Commission will, where it is practicable to do so, seek to establish other such ISPs.

13.0 Offences

13.1 It is an offence under DPA for a Board Member or an employee knowingly or recklessly, and without the Commission's consent, to obtain or disclose personal data, or to procure the disclosure the personal data to another person. The offence will not apply if the Board Member or the employee can show one of the following:

- The obtaining, disclosing or procuring of data was necessary to prevent or to detect a crime, or was required or authorised by law.

- He or she acted in the reasonable belief that he or she had the legal right to obtain, disclose or procure the data.

- He or she acted in the reasonable belief that the Commission would have consented if it had known about the obtaining, disclosing or procuring of the data.

- In the particular circumstances, the obtaining, disclosing or procuring of the data was justified as being in the public interest.

13.2 It is an offence for a Board Member or an employee to sell, or to offer to sell, personal data which have been unlawfully obtained.

14.0 Compliance

14.1 As indicated, compliance with DPA is the responsibility of all Board Members and employees. The Commission will treat any unlawful breach of any provision of DPA by any Board Member or employee as a serious matter. Any Board Member or employee who breaches this policy statement may be dealt with under the appropriate disciplinary procedure. Any such breach may also lead to criminal prosecution.

14.2 Any questions or concerns about the application of this policy statement should be referred to the HOC or the DOCS.

15.0 Training

15.1 The Commission will provide training on annual basis in the application of DPA to its employees.

16.0 Review

16.1 This policy will be reviewed annually by the HOC.

Date approved	16 August 2013
Date of last review	8 February 2016
Date of next review	8 February 2017

APPENDIX 1

GLOSSARY OF TERMS

Data mean information which

- is being processed by means of equipment operating automatically in response to instructions given for that purpose, or is recorded with the intention that it should be processed by means of such equipment – which includes both information stored in a computer and information stored so that it can be fed directly into a computer, and information stored on audio and video systems and telephone logging systems, all of which contain some element of computer control;

- is recorded as part of a relevant filing system (see below) or with the intention that it should form part of a relevant filing system;

- or forms part of an accessible record.

Personal Data mean information which relates to living individuals who can be identified from the data or from the data and other information which the organisation has or is likely to have. The term specifically includes any expression of opinion about an individual and any indication of the intentions of any person in respect of the individual.

Sensitive Personal Data mean personal data consisting of information about the following matters:

- The racial or ethnic origin of the "data subject" (see below);
- His or her political opinions;
- His or her religious beliefs or other beliefs of a similar nature;
- Whether he or she is a member of a Trade Union;
- His or her physical or mental health or condition;
- His or her sexual life;
- The commission or alleged commission by him of her of any offence; or
- Any proceedings for any offence committed or alleged to have been committed by him of her, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing, in relation to data, means obtaining, recording or holding the data or carrying out any operation on the data. It includes the organisation, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, blocking, erasure or destruction of the data.

Data Subject means the individual who is the subject of the personal data.

Data Controller means the organisation or the person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are not to be, processed.

Relevant Filing System means a set of non-automated information – that is to say, information held in manual form (for example, in paper files or non-automated micro-fiche) – relating to individuals which is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Accessible record means one of the following: a health record that consists of information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual; an educational record; or a record held by a local authority for housing or social services purposes