PFCC POLICE, FIRE AND CRIME COMMISSIONER FOR ESSEX

ESSEX POLICE
Protecting and serving Essex

Data Processing Contract

Preamble

The Police, Fire and Crime Commissioner (PFCC), as a Controller, is under a legal obligation to ensure that they process personal data in compliance with the principles of the General Data Protection Regulation (EU) 2016/679 (**GDPR**) and the Data Protection Act 2018 (**DPA**).

Where the PFCC chooses to use another organisation or person to process personal data on their behalf, that organisation or person is known as a "processor". The PFCC remains responsible for ensuring that any processor also processes personal data in compliance with those principles. Specifically, the PFCC must ensure that suitable arrangements are in place to protect the security of the personal data in question, as required by Article 28 of the GDPR, which states:

1. *Where processing is… carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures… [so] that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject…*
2. *Processing by a processor shall be governed by a contract… that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller…*

Article 28(3) of the GDPR has eight sub-paragraphs specifying particular provisions that the contract it refers to must include.

The Section 23 agreement between the Police, Fire and Crime Commissioner for Essex and Essex Police involves the processing of personal data on the PFCC's behalf by Essex Police. Consequently the contract below has been drawn up to satisfy the specific requirements of Article 28 of the GDPR.

The Contract

This Contract is made on **27th February 2020** between the parties:

The Police, Fire and Crime Commissioner for Essex, herein after called the **Controller**, of Kelvedon Park, London Road, Rivenhall, Witham, Essex, CM8 3HB (Information Commissioner Registration Number Z3451171) of the one part; and

The Chief Constable of Essex Police of PO Box No. 2, Essex Police Headquarters, Springfield, Chelmsford, Essex. CM2 6DA (Information Commissioner Registration Number Z4883472), hereinafter called the **Processor,** of the other part.

This Contract sets out the terms and conditions under which the Controller discloses Personal Data held by it to the Processor, and the Processor uses that Personal Data. Any Processing of Personal Data must comply with the provisions of this Contract.

1. Definitions

The following words and phrases used in this Contract shall have the following meanings except where the context otherwise requires:

Authorised Staff means those individuals employed by the Processor, who are authorised to process Personal Data for the purpose of the Controller's Human Resources (HR) functions, including but not limited to recruitment and payroll.

Confidential Information means all PFCC Data and any other information relating to the Controller's users and prospective users, current or projected financial or trading situations, operating plans, operating strategies, developments and all other information relating to the Controller's affairs including any trade secrets, know-how, and any information of a confidential nature imparted by the Controller to the Processor during the term of this Contract or coming into existence as a result of the Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing.

Contract means this data processing contract together with its appendices and all other documents attached to or referred to as forming part of this contract.

Data Protection Impact Assessment means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.

Data Protection Legislation means: (i) the GDPR, the LED, and any applicable national implementing laws as amended from time to time; (ii) the DPA to the extent that it relates to Processing of Personal Data and privacy; and (iii) all applicable laws relating to the Processing of Personal Data and privacy.

Data Subject, **Processing**, **Personal Data**, **Personal Data Breach**, and **Supervisory Authority** have the same meaning as in Article 4 of the GDPR.

Data Subject Rights Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted to Data Subjects pursuant to the Data Protection Legislation.

DPA means the Data Protection Act 2018.

GDPR means the General Data Protection Regulation (EU) 2016/679.

Information Asset Owner means the individual assigned, as recorded on the Information Asset Register, who is responsible for ensuring that specific information assets are handled and managed appropriately.

LED means the Law Enforcement Directive (EU) 2016/680.

NPCC means National Police Chief's Council, the replacement body for the Association of Chief Police Officers (ACPO)

Party means a party to this Contract.

PFCC Data means any data, including Personal Data and Special Categories of Personal Data, to be Processed by the Processor on behalf of the Controller under this Contract, as set out in **Appendix A: Details of data processing**.

PFCC Representative means Head of Performance and Scrutiny (Police and Crime) to the Police, Fire and Crime Commissioner for Essex, who has oversight and responsibility for ensuring the Processing on behalf of the Controller or other such person as shall be notified to the Processor from time to time complies with the terms of this Contract. The PFCC Manager will assume responsibility for co-ordinating data protection compliance, notification, security, confidentiality, audit and co-ordination of Data Subject rights and Freedom of Information requests, as directed by the terms of this Contract.

Police Manager means the Director of Human Resources for Essex Police, who has management responsibility for the Processing and compliance with this Contract on behalf of the Processor or such other person as shall be notified to the Controller from time to time. The Police Manager will assume responsibility for data protection compliance, notification, security, confidentiality, audit and co-ordination of Data Subject rights and Freedom of Information requests as directed by the terms of this Contract.

Protective Measures means appropriate technical and organisational measures to ensure a level of security of Personal Data appropriate to the risk of Processing, in accordance with Data Protection Legislation.

Purpose means the purpose of the Processing as set out in **Appendix A: Details of data processing**.

Recruitment Vetting means the NPCC vetting designed to counter a specific threat who have access to criminal intelligence, financial or operational police assets. NPCC vetting consists of **Recruitment Vetting (RV)**, Management Vetting (MV) and Non-police Personnel Vetting (NPPV).

Services means the Processing activity and services to be undertaken by the Processor on behalf of the Controller, as identified in **Appendix A: Details of data processing**.

Special Categories of Personal Data means those categories of Personal Data set out in Article 9(1) of the GDPR.

Third Country means any country that is not the United Kingdom or a member of the European Economic Area from time to time.

2. Compliance with law, the Purpose and the Controller's instructions

The details of the Processing of PFCC Data envisaged by this Contract are set out in Appendix A, and the Processor shall only process PFCC Data in accordance with Appendix A. Where deviation from Appendix A is required, this will only occur where previously authorised in writing by the PFCC Representative to the Processor.

The Processor shall process the PFCC Data:

a) in accordance with the Data Protection Legislation;

b) only for the Purpose; and

c) only on the documented instructions of the Controller, as outlined in Appendix A.

The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

The Processor shall:

d) pay any data protection fees to, and/or register any data processing particulars with, any Supervisory Authority as required by the Data Protection Legislation;

e) designate a data protection officer if required by the Data Protection Legislation; and

f) maintain complete and accurate records and information of its Processing of PFCC Data.

The Purpose is consistent with the original purpose of the Personal Data creation and/or collection, which assists the Controller in fulfilling their obligations to protect life and property, preserve order, prevent the commission of offences, bring offenders to justice, and any duty or responsibility arising from common or statute law.

Controllership of the PFCC Data shall at all times remain with the Controller.

3. Access to the PFCC Data

Access to the PFCC Data will be restricted to the Authorised Staff. The Processor will take all reasonable steps to ensure the reliability and integrity of the Authorised Staff and will ensure that the Authorised Staff:

a) are vetted by the Processor to a minimum standard of 'Recruitment Vetting' (RV) – a declaration of confidentiality is agreed to as part of this vetting process[1];

b) are aware of and comply with the Processor's duties under this Contract;

c) are informed of the confidential nature of the PFCC Data and do not publish, disclose or divulge any PFCC Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and

d) have undergone adequate training in the use, care, protection and handling of Personal Data.

4. Security of PFCC Data

The Processor recognises that the Controller has obligations relating to the security of data in their control under the Data Protection Legislation. The Processor will continue to apply those relevant obligations as detailed below on behalf of the Controller during the term of this Contract and will assist the Controller in complying with the Controller's security obligations under the Data Protection Legislation.

The Processor shall ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller, to protect PFCC Data against a Personal Data Breach, taking into account:

a) the nature of the PFCC Data;

b) the harm that might result from a Personal Data Breach;

c) the state of technological development; and

d) the cost of implementing measures.

The Protective Measures shall include, as a minimum, those measures set out in **Appendix B: Baseline Security Requirements**. In particular, the Data Processor shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport;
- deter deliberate compromise or opportunist attack; and

[1] Section 13 of Essex Police's Vetting Form (Corporate Vetting)

- promote discretion in order to avoid unauthorised access.

During the term of this Contract, the relevant Information Asset Owner of the Processor shall carry out any checks as are reasonably necessary to ensure that the above arrangements are not compromised.

The Controller will undertake any suitability checks on any persons having access to PFCC premises and the PFCC Data and further reserves the right to issue instructions that particular individuals shall not be able to participate in the Purpose without reasons being given for this decision. The Processor will ensure that each person who will participate in the Purpose understands this and will provide all required assistance to enable the Controller to exercise its rights under this provision.

The Controller reserves the right to undertake a review of security provided by any Processor and may request reasonable access during normal working hours to the Processor's premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures will result in the termination of this Contract.

5. Sub-processors

Before allowing any third-party Processor (a **Sub-processor**) to Process PFCC Data, the Processor must:

a) notify the Controller in writing of the intended Sub-processor and the Processing intended to be carried out by that Sub-processor;

b) obtain the Controller's written consent to the use of that Sub-processor;

c) enter into a written contract with the Sub-processor imposing on the Sub-processor terms that are substantially equivalent to those set out in this Contract in respect of the PFCC Data; and

d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

6. Transfers to Third Countries

The Processor shall not transfer PFCC Data to a Third Country unless the Controller's prior written consent is obtained and the following conditions are fulfilled:

a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer in accordance with the Data Protection Legislation, as determined by the Controller;

b) the Data Subject has enforceable rights and effective legal remedies;

c) the Processor complies with its obligations under the Data Protection Legislation in respect of such transfer; and

d) the Processor complies with any reasonable instructions notified to it by the Controller with respect to the transfer.

7. Data Subject Rights Requests

The Processor shall:

a) notify the Controller immediately (and in any event within two business days) if it receives a Data Subject Rights Request (or purported Data Subject Rights Request) relating to the PFCC Data;

b) provide the Controller with full details and copies of the Data Subject Rights Request; and

c) provide full assistance to the Controller to enable the Controller to comply with a Data Subject Rights Request within the relevant timescales set out in the Data Protection Legislation.

8. Personal Data Breaches and data protection communications

The Processor shall:

a) notify the Controller immediately (and in any event within 24 hours) upon becoming aware of a Personal Data Breach affecting the PFCC Data, including full details of the Personal Data Breach;

b) notify the Controller immediately (and in any event within two business days) if it receives any claim, request, complaint, notification or communication from a Data Subject, Supervisory Authority or another third party relating to either Party's Processing of the PFCC Data (a **Data Protection Communication**) and provide the Controller will full details and copies of the Data Protection Communication; and

c) provide the Controller will full assistance following any Personal Data Breach or the receipt of any Data Protection Communication to enable the Controller to handle such Personal Data Breach or Data Protection Communication in accordance with the Controller's obligations under Data Protection Legislation.

The Processor shall not contact any Data Subject directly or respond to a Data Subject Rights Request or Data Protection Communication without the Controller's prior written consent or as permitted by Appendix A.

The Processor's obligations to notify the Controller under this clause 8 shall include an obligation to provide further information to the Controller in phases, as details become available, if full information is not available at the time of notification.

9. Data Protection Impact Assessments

The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment relating to the Processing of the PFCC Data. Such assistance may, at the discretion of the Controller, include:

a) assisting the Controller in preparing a systematic description of the envisaged Processing operations and the Purpose;

b) assisting the Controller in conducting an assessment of: i) the necessity and proportionality of the Processing operations in relation to the Purpose; and ii) the risks to the rights and freedoms of Data Subjects; and

c) providing the Controller with full information about the Protective Measures in place.

The Processor shall provide all reasonable assistance to the Controller in complying with the Controller's obligations to carry out prior consultation with a Supervisory Authority in accordance with the Data Protection Legislation.

10. Retention, Review and Deletion

The PFCC Data will be retained by the Processor, and any agreed Sub-Processors, and then securely disposed when no longer required for the Purpose, in accordance with Appendix A. In any event, on termination of the Contract, the Processor, and any agreed Sub-Processors, shall, at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller unless required by law to retain the Personal Data.

11. Audit

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations in this Contract and shall allow for and

Signed on behalf of the Police, Fire and Crime Commissioner, by:

JEGardner

Print Name: JANE GARDNER

Date: 3 MARCH 2020

Signed on behalf of the Chief Constable, Essex Police by:

Print Name: Richard Leicester

Date: 28/02/2020

reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it.

The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

[Signature blocks appear on the next page]

In the event of any dispute or difference arising between the Parties out of this Contract, the PFCC Manager and the Police Manager shall meet in an effort to resolve the dispute or difference in good faith.

The Parties will, with the help of the Centre for Effective Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

16. Term and termination

The Purpose, as outlined in Appendix A, is for the Processor to provide HR and IT function and support to the Controller, as such this Purpose is ongoing. The Contract will stand whilst the role of PFCC for Essex remains, or until the PFCC identifies alternative arrangements for the provision of either service.

The Controller may at any time by notice in writing terminate this Contract forthwith if the Processor is in material breach of any obligation under this Contract.

Either Party may terminate this Contract by giving 30 days' notice in writing to the other Party.

Notwithstanding termination of this Contract, clauses 2 to 15 of this Contract shall survive termination to the extent that the Processor continues to Process PFCC Data on behalf of the Controller.

17. Variation

The Controller will have the final decision on any proposed variation to this Contract. No variation of the Contract shall be effective unless it is contained in a written instrument signed by both Parties and annexed to this Contract, save that:

a) the Controller may, at any time on not less than 30 business days' notice, revise this Contract by replacing all or part of it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract); and

b) the Parties agree to take account of any guidance issued by any relevant Supervisory Authority and the Controller may, on not less than 30 business days' notice, amend this Contract to ensure that it complies with any guidance issued by a relevant Supervisory Authority.

18. Miscellaneous

This Contract acts in fulfilment of part of the responsibilities of the Controller as required by Article 28 of the GDPR.

This Contract constitutes the entire agreement between the Parties as regards its subject matter and supersedes all prior oral or written agreements regarding such subject matter.

If any provision of this Contract is held by a court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Contract, which shall remain in full force and effect.

The validity, construction and interpretation of the Contract and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

Headings are inserted for convenience only and shall not affect the construction or interpretation of this Contract and, unless otherwise stated, references to clauses and appendices are references to the clauses of and appendices to this Contract.

Any reference to any enactment or statutory provision shall be deemed to include a contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

Upon request, the Processor shall allow the Controller, any relevant Supervisory Authority and their representatives access to its premises, records and personnel for the purpose of assessing the Processor's compliance with its obligations under this Contract.

12. Human Rights

The processing of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Contract by the Data Protection Legislation and the Human Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the Parties to this Contract.

The Parties agree and declare that the information accessed pursuant to this Contract will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportionate, having regard to the purposes of the Contract and the steps taken in respect of maintaining a high degree of security and confidentiality.

If any Party to this Contract receives a request for information under the provisions of the Freedom of Information Act 2000 identified as originating from another Party, the receiving Party will contact the other Party to determine whether the latter wishes to claim an exemption under the provisions of that Act.

13. Confidentiality

The Processor shall not divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or with the prior written authority of the Controller) any Confidential Information, which it shall treat as private and confidential and safeguard accordingly. The restriction in this paragraph shall not apply where disclosure of the Confidential Information is ordered by a court of competent jurisdiction or is otherwise required by any law or regulation to which the Processor is subject. In such a case, the Processor shall immediately notify the Controller in writing of any such requirement for disclosure of the Confidential Information in order to allow the Controller to make representations to the person or body making the request.

The Processor shall ensure that only Authorised Staff have access to Confidential Information under this Contract, and are aware of their responsibilities in connection with the use of that Confidential Information.

For the avoidance of doubt, the obligations of confidentiality imposed on the Parties by this Contract shall continue in full force and effect after the expiry or termination of this Contract.

The restrictions contained within this section 13 shall cease to apply to any information which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Contract.

14. Indemnity

In consideration of the provision of the PFCC Data for the Purpose the Processor undertakes to indemnify and keep indemnified the Controller against any liability which may be incurred by the Controller as a result of the Processor's breach of this Contract, provided that this indemnity shall not apply to the extent that the liability arises from information supplied by the Controller which is shown to have been incomplete or incorrect, unless the Controller establishes that the error did not result from any wilful wrongdoing or negligence on their part.

15. Disputes

Appendix A: Details of Data Processing

The Processor shall comply with any further written instructions with respect to Processing from the Controller.

Any such further instructions shall be incorporated into this Appendix.

Subject matter of the Processing	i. Human Resources (HR) function, including but not limited to payroll and recruitment on behalf of the PFCC. ii. Provision of IT Services through access to the Essex Police IT Infrastructure
Duration of the Processing	The arrangement is ongoing whilst the office of the PFCC remains in place or until the PFCC identifies alternative arrangements for the provision or either service.
Purposes of the Processing	i. HR function for the purpose of replicating the services provided to Essex Police employees for the benefit of those employed by the PFCC. ii. Provides the PFCC with an IT infrastructure for the PFCC's own organisational purposes, including use of email, intranet, extranet and internet in accordance with section 9 of the Information Sharing Agreement between Essex Police and the Police, Fire and Crime Commissioner for Essex, dated November 2018 and signed by the PFCC (4.12.18) and Chief Constable (23.11.18)
Nature of the Processing	i. HR function for the purpose of replicating the services provided to Essex Police employees for the benefit of those employed by the PFCC. ii. Provides the PFCC with an IT infrastructure for the PFCC's own organisational purposes, including use of email, intranet, extranet and internet in accordance with section 9 of the Information Sharing Agreement between Essex Police and the Police, Fire and Crime Commissioner for Essex, dated November 2018 and signed by the PFCC (4.12.18) and Chief Constable (23.11.18) Signed ISA Dec 2018 PFCC and EP.p
Type of Personal Data	i. HR related data, including but not limited to: name, address, telephone numbers, date of birth, next of kin, ethnicity*, nationality, gender, marital status, personal development review, bank details, payslip, National Insurance details, annual leave, sickness, job history, ii. All categories of police and PFCC data stored or processed through the Essex Police IT infrastructure. *Special category personal data

Categories of Data Subject	All employees of the Police, Fire and Crime Commissioner for Essex
Arrangements for return or destruction of the data once processing is complete	In accordance with the following Essex Police Policies and Procedures: W1000 Policy – Information Management and Assurance. W1012 Procedure – Records Review, Retention and Disposal.
Authorised Staff	i. Staff under the responsibility of the Director of Human Resources, Learning and Development [for both Essex and Kent Police] – Essex Police. ii. ITD staff – Essex Police

Appendix B: Baseline Security Requirements for Data Processing Contracts

Introduction

All Chief Constables are committed to compliance with the NPCC Security Systems Policy, which was based on the British Standard for Information Security Management (BS7799), now superseded by ISO 27001.

Section 1 Information Security Policy

A written statement of Information security policy should be available for the organisations involved in the Contract.

All staff of the Processor are subject to the Essex Police's set policies and procedures, including those relating to Information Security, comprising of: W1001; W1002; W1004; W1006; W1008; W1009; W1016; W1017; W1020; W1021; W2006; W2011; W2013

W 2013 Procedure -
Appropriate Access ar

Section 2 Information Security Organisation

Responsibility for information security should be allocated to an individual within the organisation. That individual should be operating within a management framework that initiates and controls the implementation of information security:

Anna Hook - Head of Performance and Scrutiny (Police and Crime), Data Protection Officer. Police, Fire and Crime Commissioner for Essex
James Wyatt – Essex Police Information Security Officer

Section 3 Assets Classification and Control

It is important to maintain appropriate protection of the computer and information assets used by the data processor. The below lists the hardware, software and information, which will be used for the purposes of the Contract:

Essex Police IT Infrastructure

Accountability for these assets for the purpose of the Contract is with:

Information Asset Owners – please refer to Essex Police's Information Asset Register

Section 4 Personnel Security

The Controller will need to ensure the reliability of any persons having access to data.

How has the reliability of persons subject to this Contract *been assessed?*

Statutory working relationship between the PFCC for Essex and Essex Police established under the Police Reform and Social Responsibility Act and Statutory Instrument 2011 No. 2744 'The Policing Protocol Order 2011'.

Any persons having access to data as part of this Contract *may be required to give consent to background enquiries in accordance with policy. Please provide written consent as required.*

All staff of the Controller and Processor (PFCC and Police) are vetted as a matter of routine, this Contract set as a minimum standard of NPCC vetting of Recruitment Vetting (RV). No separate authorisation or consent is sought under the understanding that accessing data by the Processor is authorised only in the exercise of their employed duties, and is governed by documented policy and procedures.

Please confirm that all persons connected with these processes have received training and awareness in Data Protection and information security.

All staff of the Processor are mandated to undertake Data Protection and Information Security training. These are available under 'Data Safe' in the Develop Me application.

1. Data Protection 2018
2. Data Protection 2018 Refresher
3. Information Security

Please confirm that all persons involved with these processes are made aware of the procedure for reporting any security breaches, threats, weaknesses of malfunctions that might impact on the security of the data.

All staff of the Processor are aware of the Information Breach process as contained within W1004 Procedure – Incident Reporting and Management.
This is reinforced by completion of the Information Security Training Package.

Section 5 Physical and Environmental Security

Appropriate measures should be in place to prevent unauthorised access or unlawful processing, accidental loss, destruction or damage.

Please advise details of the premises used for this purpose and in relation to each named premises:-

Whilst the following questions have been briefly answered, the work being undertaken is on *police premises or under remote working arrangements. All PFCC data and processes to support the work is undertaken under the same controls as Essex Police operates for its own processes and data security.*

a) What access controls are there to the buildings?	All premises are access controlled
b) What access controls are there to the rooms?	Premises are access controlled with some rooms subject to further access controls.
c) Are the windows lockable when accessible from the outside?	Yes
d) Is the door lockable where the information is stored?	Yes
e) Is information secured in a lockable cabinet when not in use?	Yes
f) Is there a clear desk policy in relation to this information?	Yes
g) Do outside contractors/ maintenance/cleaning staff have access to the room?	Yes
h) Is the information visible to unauthorised individuals, i.e., through windows, from corridors etc.	No
i) Is there any intention to use portable computers for this purpose? If so, what special control measures will be deployed to protect data?	Yes. Essex Police security arrangements are in place for all portable IT equipment.
j) Is the computer/server used to store data in connection with the process physically secured in any way (e.g. by cable to desk etc.)?	Yes

Section 6 Computer and Network Management

In addition to the physical security outlined above, please provide details of the following:-

Whilst the following questions have been briefly answered, the work being undertaken is on police premises or under remote working arrangements. All PFCC data and processes to support the work is undertaken under the same controls as Essex Police operates for its own processes and data security

a) Is the computer a stand-alone? If not, what measures are taken to prevent unauthorised access via your network or from external networks?	Varies. All IT is subject to Essex Police security processes.
b) Is there a policy and procedure for the disposal of sensitive material (computer or otherwise)? What procedure is in place to ensure that the data is cleansed from computer media as it becomes obsolete for whatever reason? What procedure is in place to ensure that data held on computer media is handled appropriately when equipment is sent for repair?	Yes: W1012 Procedure - Records Review, Retention and Disposal. W1016 Procedure – Encryption of Files and Removable Data. W4001 Procedure – IT Access Management W4004 Procedure – Disposal of IT Equipment
c) Are system security procedures regularly audited?	Yes
d) Are there documented rules for the use of this system available for all users? If so, do users sign to show they have read and understood the Rules?	Yes
e) What control measures are in place to prevent the introduction of malicious software to the system (e.g., computer viruses)?	Essex Police ITD manages IT security protection. PFCC data will be subject to identical security arrangements as Essex Police systems and data.

Section 7 System Access Controls

a) Are there controls on the system to prevent unauthorised access (i.e. Is there a mechanism for the identification and authorisation of individual users, e.g., user ID and password)?	Yes
b) Is there an automatic log-out after an appropriate time interval?	Yes
c) Is there a warning at log-on to forbid unauthorised use of the system?	Yes
d) Is there an audit trail to identify who has accessed the system including time, date and which records were accessed?	Yes
e) Who monitors the audit trails? How long are they retained and how is the security of the audit trails maintained?	ITD and Information Security. Access and audit are covered in: W4001 Procedure – IT Access Management

Section 8 Systems Development and Maintenance

All information systems used as part of this Contract should be designed from the outset with information security in mind to cover, as a minimum, the control measures contained in this document.

Section 9 Business Continuity Planning

a) Is there an effective backup and recovery mechanism to secure the data? And, where is this held?	Yes – Essex Police Estate
b) What security surrounds these backup facilities?	Essex Police Security Arrangements