Processing Agreement

Between

“Rushcliffe Borough Council"

And

“Broxtowe, Newark and Sherwood and Ashfield Surveillance Camera Systems Partnership”

1. Parties

The Parties to this Agreement are:

(a) **Rushcliffe Borough Council,** Council Offices, Rushcliffe Arena Rugby Rd, West Bridgford, Nottingham NG2 7HY ("**the Council**"); and

(b) **"Contractor – Service Provider",** Broxtowe, Newark and Sherwood and Ashfield Surveillance Camera Systems Partnership ("**the Service Provider**").

2. Introduction

2.1 Rushcliffe Borough Council require the Service Provider to process Surveillance information and personal data on behalf of the Council. The Council carry out surveillance monitoring throughout the Borough of Rushcliffe, predominately within its main town centres, West Bridgford, and surrounding areas, whereby it monitors, records and retains surveillance images of a personal nature and stores these images under its obligation to perform a public task in pursuance of public protection. ("the Council") has a statutory duty to meet its obligations as set out within the Data Protection Legislation 2018 (DPA 2018), the UK General Data Protection Regulations in its operation of overt surveillance camera systems in public places by local authorities in England and Wales and Section 33(1) of the Protection of Freedoms Act 2012

2.2 This Agreement is to ensure the protection and security of data passed from the Council to the Service Provider for Processing or data accessed by the Service Provider on behalf of the Council for Processing or otherwise received by the Service Provider for Processing on the Council's behalf;

2.3 The UK GDPR place certain obligations upon a Controller to ensure that any Processor it engages provides sufficient guarantees to ensure that the Processing of the data carried out on its behalf is secure and protects the rights of the Data Subject;

2.4 This Agreement exists to ensure that there are sufficient security guarantees in place and that the Processing carried out by the Processor on the Controller's behalf complies with obligations under Article 28 of the UK GDPR;

2.5 This Agreement further defines certain service levels to be applied to all data related services provided by the Processor.

3. Definitions

In this agreement;

Agreement: this contract.

Data Protection Legislation: (i) the UK GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; all applicable Law about the processing of personal data and privacy.

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

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach. Data Subject Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

Data Subject Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

DPA 2018: Data Protection Act 2018

Controller, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer** and **Processing** shall have the same meanings as assigned to those terms in the UK GDPR;

Good Industry Practice: means in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgement that would reasonably be expected from a skilled person engaged in the same type of undertaking under the same or similar circumstances;

GDPR: the UK General Data Protection Regulation (Regulation (EU) 2016/679)

Law: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

Party: a party to this agreement

Processor Personnel: means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in this agreement.

The Supplier's Personnel: all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-processor engaged in the performance of its obligations under this Agreement;

Sub-processor: any third Party appointed to process Personal Data on behalf of that Processor related to this agreement.

4. Application of this Agreement

This Agreement shall apply to:

4.1 All Data sent by the Council to the Service Provider for Processing is in exercise of its powers as a relevant authority. A relevant authority must have regard to the surveillance camera code of practice when exercising any functions to which the code relates, for such systems, in accordance with the Information Commissioners Officer (ICO) and the Surveillance Camera Commissioners Office (SCC). Surveillance camera systems which relevant authorities operates within the scope of the Protection of Freedoms Act 2012 (PoFA) and whether you comply with the provisions of Section 33 of PoFA.

4.2 All Data accessed by the Service Provider on authorisation of the Council for Processing purposes is in exercise of its powers scope of the Protection of Freedoms Act 2012 (PoFA) and whether you comply with the provisions of Section 33 of PoFA. All Data otherwise received by the Service Provider for Processing purposes on the Council's behalf in exercise of its powers as a relevant authority in accordance with the Local Government Act 1972 is a relevant authority carrying out surveillance using surveillance cameras which have meaning given by Section 29(6) of the 2012 Act and is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained

5. Data Processing

5.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Council is the Controller and the Service Provider is the Processor unless otherwise specified in Schedule 1. The only processing that the Processor is authorised to do is listed in Schedule 1 by the Controller and may not be determined by the Processor.

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

5.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data. More detail on security measures to have in place are detailed in Annex B.

5.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule 1 unless the Processor is required to do otherwise by Law. If it is so required, the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
    (i) nature of the data to be protected;
    (ii) harm that might result from a Data Loss Event;
    (iii) state of technological development; and
    (iv) cost of implementing any measures;

(c) ensure that the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 1);

(d) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
  (i) are aware of and comply with the Processor's duties under this clause;
  (ii) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
  (iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
  (iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(e) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
  (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 44 and 46) as determined by the Controller;
  (ii) the Data Subject has enforceable rights and effective legal remedies;
  (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(f) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

5.5 Subject to clause 5.6, the Processor shall notify the Controller immediately if it:
(a) receives a Data Subject Request (or purported Data Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

5.6 The Processor's obligation to notify under clause 5.5 shall include the provision of further information to the Controller in phases, as details become available.

5.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 5.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach;

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

5.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the processing is not occasional;

(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or

Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

5.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

5.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

5.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause such that they apply to the Sub-processor; and

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

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

5.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing 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 Agreement).

5.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

5.15 For the purposes of this Agreement, the provisions that provide the legal basis for this processing of Personal Data under Article 6(1) of GDPR are listed below:

(a) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

6. Data to be provided by the Council

6.1 The Council will only provide Data which is relevant to the purpose outlined in **Annex A - Schedule**. The Council will not provide any Data it considers to be irrelevant or excessive.

6.2 The Data provided by the Council under this Agreement is Personal Data as defined by the Data Protection Legislation.

6.3 Data will be provided for the specific purpose set out in the **Annex A - Schedule.**

6.4 All intellectual property rights in the Data shall belong to the Council. The Data shall be identified, clearly recorded and marked as such by the Service Provider on all media and in all documentation.

7. Obligations of the Service Provider

7.1 All information and data coming into possession of the Service Provider will be treated in the strictest confidence and in accordance with the General Data Protection Regulation and associated Data Protection Legislation and the Freedom of Information Act 2000.

7.2 The Service Provider represents the Council and therefore is to act in the interest of the Council at all times, providing a professional service.

7.3 The Service Provider agrees that it shall ensure that it complies at all times with the Data Protection Legislation, and, in particular, the Supplier shall ensure that any disclosure of Personal Data made by it to the Council is made with the Data Subject's consent or is otherwise lawful.

8. Termination

8.1 This Agreement shall terminate automatically upon termination or expiry of the Service Providers obligations in relation to the Services and, on termination of this Agreement, the Service Provider shall forthwith deliver to the Council as described by the Council in Annex 1 - Schedule all the Service Providers Data in its possession or under its control. Upon verification of receipt of this data the Service Provider will securely destroy any copies of this data in their possession (subject to any mandatory retention periods).

8.2 Clause 8.1 is subject to the statutory requirements of retention of Data as legally required.

8.3 The Council shall be entitled to terminate this Agreement forthwith by notice in writing to the Service Provider if the Service Provider is in material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within twenty-one (21) days from the date of receipt by the Service Provider of a notice from the Council identifying the breach and requiring its remedy.

8.4 The Parties may terminate this Agreement on agreement or by one Party giving the other Party 1 (one) months' written notice to terminate the Agreement.

8.5 Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination of this Agreement shall remain in full force and effect.

9. Waiver

Failure by either Party to exercise or enforce any rights available to that Party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of that party's rights under this Agreement.

10. Invalidity

If any term or provision of this Agreement shall be held to be illegal or unenforceable in whole or in part under any enactment or rule of law such term or provision or part shall to that extent be deemed not to form part of this Agreement. However, the enforceability of the remainder of this Agreement shall not be affected provided that if any term or provision or part of this Agreement is severed as illegal or unenforceable, the Parties shall seek to agree to modify this Agreement to the extent necessary to render it lawful and enforceable and, as nearly as possible, to reflect the intentions of the Parties embodied in this Agreement including without limitation the illegal or unenforceable term or provision or part.

11. Entire Agreement

11.1 This Agreement and the documents attached to or referred to in this Agreement shall constitute the entire understanding between the Parties and shall supersede all prior Agreements, negotiations and discussions between the Parties. In particular, the Parties warrant and represent to each other that in entering into this Agreement they have not relied upon any statement of fact or opinion made by the other, its officers or agents which has not been included expressly in this Agreement. Further, each Party hereby irrevocably and unconditionally waives any right it may have:

11.2 to rescind this Agreement by virtue of any misrepresentation;

11.3 to claim damages for any misrepresentation whether or not contained in this Agreement;

11.4 save in each case where such misrepresentation or warranty was made fraudulently.

12. Indemnities

Each Party shall indemnify the other Party/Parties against all liabilities, costs, expenses, damages and losses (including but not limited to any

direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) administrative fines and losses from data subject claims and all other reasonable professional costs and expenses) suffered or incurred by the indemnified Party/Parties arising out of or in connection with the breach of the Data Protection Legislation by the indemnifying Party, its employees or agents, provided that the indemnified Party/Parties gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

The Service Provider shall indemnify (and keep indemnified) the Council any action, proceeding, liability, cost, claim, loss, monetary penalty, expense (including reasonable legal fees and disbursements) and demands incurred by the Council which arise directly through any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with any part of the Data Protection Legislation by the Service Provider or its employees, agents or sub-contractors.

13. Notices

13.1 Notices shall be in writing and shall be sent to the other Party marked for the attention of the person at the address set out in this Agreement. Notices may be sent by first-class mail or electronic mail. Correctly addressed notices sent by first-class mail shall be deemed to have been delivered 2 (two) working days after posting and correctly directed electronic mail shall be deemed to have been delivered 24 (twenty) hours after transmission.

13.2 No notice is deemed to have been received unless it is sent to the designated officer as detailed in **Annex A**.

14. Third Party Rights

A person who is not a Party to this Agreement has no rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any terms of this Agreement.

15. Governing Law

This Agreement will be governed by the laws of England, and the parties submit to the exclusive jurisdiction of the English courts for all purposes connected with this Agreement, including the enforcement of any award or judgement made under or in connection with it.

16. Data Retention and Deletion

Any Shared Personal Data must only be retained for as long as strictly necessary for the purposes of the sharing/processing set out in Annex A Schedule 1. Each Party shall regularly review the information held by it to ensure that retention of the shared/processed personal data is still

required for the stated purpose; any information that no longer needs to be retained shall be securely deleted by the relevant officer. Any such review of the shared/processed personal data must be conducted in accordance with the relevant Party's document retention policy, as amended from time to time. (For the avoidance of the doubt, the relevant Party for the purpose of this clause shall be the Party that holds the particular shared/processed personal data.)

17. Freedom of Information (FOI) Requests

Requests covered by the Freedom of Information Act 2000 are requests for recorded information held by a public authority that is not personal. If a Party receives a FOI request and the data is identified as belonging to that Party, it will be the responsibility of the lead contact in section 1 for that Party to contact the other Party/Parties, usually the lead contact in section 1 who will take the lead as far as the request is concerned. Communication must take place speedily thus allowing the servicing of the request to take place within the statutory 20-day time period.

18. Review Date

Each Party shall review this agreement every 12 months to ascertain whether the information sharing initiative is still required. If the information sharing is no longer required, this agreement should be terminated in accordance with clause 8 (Termination of or withdrawal from this agreement).

This Agreement has been entered into on the date stated at the beginning of it.

Signed by for and on behalf of
RUSHCLIFFE BOROUGH COUNICL .....
Authorised signatory

Mr G Carpenter
Service Manager (Public Protection) - Neighbourhoods

Signed by for and on behalf of
"CONTRACTOR" .....
Authorised signatory

The Council will retain a signed copy of this agreement to show that both parties fully accept their responsibilities.

ANNEX A – Schedule 1 Processing, Personal Data and Data Subjects

This schedule shall be completed by the Council, who may take account of the view of the Service Provider, however the final decision as to the content of this Schedule shall be with the Council at its absolute discretion.

1. The contact details of the designated persons:
   Name: Derek Musto
   Role: Parking, CCTV and Security Manager (SPOC)
   Email: derek.musto@Rushcliffe.gov.uk
   Tel: 01159173620

2. The contact details of the Data Protection Officer:
   Name: Greg Dwyer
   Role: Chief Information Officer
   Email: greg.dwyer@rushcliffe.gov.uk
   Tel: 01159148411

3. The Service Provider shall comply with any further written instructions with respect to processing or sharing data on behalf of the Council.

4. Any such further instructions shall be incorporated into this Schedule

Description	**Details**
Subject matter of the processing (what type of information)	• Vehicle registration details • Vehicle location • Surveillance information • Crime and assist in the detection of criminal offences • Anti-social behaviour and assist in the detection of anti-social behaviour incidents • Visitors and the business community who use the facilities covered by the surveillance scheme • Assisting the emergency services in the location of Missing Vulnerable persons. • Personal information in relation to third party disclosure requests • Personal information in relation to subject access requests • Personal information in relation to authorised RIPA requests
Duration of the processing (how long is the contract)	Until termination of this agreement all personal data processing must immediately cease.
Nature and purpose of the processing (why do we need to process the information)	**Processing of Personal Data** Article 6(1)(c) UK GDPR: The processing of surveillance data/information and images is necessary for local authorities and the Police to comply with its legal and lawful obligations. Local authorities establish their

	Surveillance Camera Systems under the UK GDPR/DPA 2018 and Section 17 Crime and Disorder Act 1998 which places a legal obligation on local authorities and the police to work in partnership to develop and implement a strategy for tackling crime and disorder. In addition, Section 163 of the Criminal Justice and Public Order Act 1994 creates the legal powers for local authorities to provide surveillance camera coverage of any land within their area for the purposes of crime prevention or victim welfare. Article (e) of GDPR: The processing is also necessary for the performance of a task carried out in the public interest - crime prevention and detection of criminal offences. **Special Category Data** Article 9(2) (g) of GDPR: The processing of surveillance information, data and images is necessary for substantial public interest reasons of crime detection and prevention as prescribed under Para.10 of Pt. 2 to Sch.1 of UK Data Protection Act 2018 (DPA18) **Criminal Data** Part 3 of DPA 18: The processing of surveillance information, data and images is necessary for the prescribed “law enforcement purposes”: Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties referenced under Para 31 to Part.3 of the Act. Where the council processes data for the law enforcement purposes they do so as a “data controller” as defined under Para 32 to Pt.3 of the Act. **For Police Constabularies processing of personal information and data:** The processing of information, data and images is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, “law enforcement purposes”, as referenced under Para. 31 to Part 3 of DPA 2018. Where police process personal information, data and surveillance images is for the prescribed law enforcement purposes, we do so acting as a competent authority and in the exercise of their official authority as referenced under Part 3 of DPA18. (i) Non– Law

	Enforcement purposes: preventing or detecting unlawful acts (ii) Law Enforcement Purposes: Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
Type of personal data (what type)	• Personal data in the form of video • Associated written personal data • Sensitive data • Category data • Criminal information/data • Video badge footage/screenshots • Third party details (witness statements) • Vehicle keeper details
Categories of personal data (do any of these apply) race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.	The Council will in the interest of public safety process personal data of persons in public places such as town centre areas, car parks, recreation areas, the internal and external areas of public buildings. The data collected and processed is in the form of recorded video footage and accompanying documentation. There may be images of children, vulnerable persons, people from minority ethnic groups and religious beliefs, however this will not be known at the time of recording/processing unless the information is made available by the appropriate authorities or enforcement agencies, personal data would relate to: • Victims • Offenders • Witnesses • Public
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Any stored material will be retained for 30 days, standard retention on the main system data storage media, deleted automatically if no request for disclosure in made within that period. If a formal disclosure request is made the data will be archived in an evidence locker for a further 30 days (60 days in total) if it is no longer relevant to a live or ongoing investigation after which all achieved data will be deleted. This is deemed by the Council to be a sufficient amount of time for enforcement agencies (including the Police) to carry out their investigations and make a formal export data request. All archived/quarantined footage/images processed will be deleted unconditionally after 60 days from initial archiving, unless directly associated with an ongoing criminal investigation or criminal prosecution where a formal request has been made for the

	Council to retain footage as evidence for longer than deemed necessary under normal Council policy. A separate data privacy impact assessment will be completed justifying an extended retention period where necessary. Where any archived/quarantined footage has been disclosed to enforcement agencies (including the Police), it will be deleted after the initial 30/60 days' retention as part of the disclosure process, handing over responsibility of any master copies and transferring liability for data control/processing to that agency under the formal disclosure process. This handover of responsibility/transfer of liability will be documented. • Surveillance control room live monitoring 24/7 (no audio or facial recognition will be recorded) • Surveillance recording 24/7 held on encrypted digital servers within the camera control room • Information/data is stored for 30 days unless associated with an ongoing criminal investigation • Stored footage reviewed by request only (incidents) after completion of a formal designated third party disclosure form (including the police) • Subject access requests satisfied only by completion of the Council's subject access form • If data or information is relevant and of evidential value or of subject relevance, material burnt to DVD transferring liability or responsibility for data control and processing to appropriate agency • Disc only handed over after completion of a liability transfer document identifying the holder as the data controller and responsible for its processing under the DPA 2018 and the GDPR 2016. • Data is automatically overwritten, destroyed/deleted after 30/60 days unless an exemption applies

This Data Processing Schedule may be amended at any time during the period of the Contract, by agreement in writing between the Council and the Service Provider to ensure that the description and detail set out in the data processing schedule with regard to the processing of Personal Data reflects the arrangements between the parties, is accurate and is compliant with the Data Protection Legislation.

Annex B – Minimum Information Security Controls

General

A security policy must be in place which sets out management commitment to information security, defines information security responsibilities, and ensures appropriate governance.

All staff must complete data protection and information security training commensurate with their role.

Pre-employment checks that take into account relevant employment legislation including verification of identity and right to work must be applied to all staff.

IT Infrastructure

Boundary firewall and internet gateways

Information, applications and devices must be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Secure configuration

ICT systems and devices must be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User access control

User accounts must be assigned to authorised individuals only, managed effectively, and they must provide the minimum level of access to applications, devices, networks, and data.

Access control (username & password) must be in place. A password policy must be in place which includes:

- Avoiding the use of weak or predictable passwords.
- Ensuring all default passwords are changed.
- Ensuring robust measures are in place to protect administrator passwords.
- Ensuring account lock out or throttling is in place to defend against automated guessing attacks.

End user activity must be auditable and include the identity of end-users who have accessed systems.

Malware protection

Mechanisms to identify detect and respond to malware on ICT systems and devices must be in place and must be fully licensed, supported, and have all available updates applied.

Patch Management and Vulnerability Assessment

Updates and software patches must be applied in a controlled and timely manner and must be supported by patch management policies.

You must adopt a method for gaining assurance in your organisation's vulnerability assessment and management processes, for example by undertaking regular penetration tests.

Software which is no longer supported must be removed from ICT systems and devices.

Cloud Services

You must ensure that the controls applied to the use of cloud services satisfactorily supports the relevant security principles set out in the National Cyber Security Centre Cloud Security Principles: - security-principles

Protecting Confidential Data

Electronic Data

Electronic copies of confidential data must be encrypted at rest to protect against unauthorised access.

When transmitting confidential data over the internet, over a wireless communication network e.g. Wi-Fi, or over an untrusted network you must use an encrypted communication protocol.

You must only use ICT which is under your governance and subject to the controls set out in this schedule.

Hard Copy Confidential Data

Hard copy Confidential Data must be stored securely when not in use and access to the data must be controlled.

- It must be transported in a secure manner commensurate with the impact a compromise or loss of information would have and which reduces the risk of loss or theft.

Secure Destruction of Confidential Data

Electronic copies of confidential data must be securely destroyed when no longer required. This includes data stored on servers, desktops, laptops or other hardware and media.

Hard copy information must be securely destroyed when no longer required.

Secure destruction means destroying data so it cannot be recovered or reconstituted.

A destruction certificate may be required to provide the necessary assurance that secure destruction has occurred.

Security Incidents/Personal Data Breach

You must notify the council immediately of any fact or event which results in, or has the potential to result in, the compromise, misuse, or loss of council information, ICT services or assets.

You must notify the council immediately of any personal data breach if the breach relates to personal data processed on behalf of the council.

You must fully co-operate with any investigation that the council requires as a result of such a security incident or personal data breach.

Compliance

The Council must be informed of any non-compliance with these controls. Any deficiencies in controls must be subject to a documented risk management process and where appropriate a remedial action plan is to be implemented with the aim of reducing, where possible, those deficiencies.

Independent validation which has been used as evidence of appropriate security controls must be maintained throughout the life of the contract.

The council must be made aware of any expired or revoked evidence used as independent validation.