Essex County Council

# Description of Security Measures employed to safeguard the processing of Personal Data by Essex County Council

## 1. Organisational

### a. Policies & Documented Procedures

Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Organisation's processes. All policies have documented review dates and ownership is assigned. Reviews are held ahead of the expiry date or sooner where there is an identified issue. All policies follow a governance route for approval. All relevant policies are published to the Council's intranet and a shortcut link to a dedicated landing page is made available through internet browser software. Key policies are published to the organisation's website for transparency.

### b. Roles

The organisation has a named Data Protection Officer who is Paul Turner. This Officer executes the role by reporting the outcome of statutory process to Margaret Lee who acts as the organisation's Senior Information Risk Owner (SIRO).

The Information Governance function has employees trained and qualified in Data Protection law who fulfil a number of security management functions:

1) Assessing proposals for the need to conduct Data Protection Impact Assessments (DPIA)
2) Ensuring appropriate security measures are in place through the DPIA process
3) Assessing requests for exceptions to policy and managing the review of existing exceptions
4) Drafting new and reviewing existing policy.
5) Managing the policy approval process and publishing amendments
6) Co-ordinating a network of 'Information Champions' who act as a both a consultation body to assist with policy development, and as a conduit for promoting policy, best practice and consulting on proposals for the areas of the Council which they represent.

## c. Training & Awareness

The organisation regularly reviews employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure new employees receive appropriate training before accessing personal data, and all other employees receive refresher training via mandatory eLearning courses every 2 years. All training received is documented for evidence purposes. These provisions are documented in a training strategy.

There is additional formal training and awareness-raising events delivered to Council employees particularly for Social Care services. Some events also include the employees of Data Processors and Partners in order to improve the security measures over data when shared with other bodies.

The Information Governance function develops and delivers a communications plan which seeks to promote good Data Protection practice with regular messages to employees. This is supplemented by reactive messages in response to specific incidents and proactive messages where there are known threats.

The Council uses a desktop tool which periodically requires employees to read and confirm understanding of policies or key messages. This is recorded for evidential purposes

## d. Risk Management & Privacy by Design

The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership and rated against a consistent schema. Appropriate mitigations are identified and are reviewed monthly.

The Information Governance function assesses proposals for new (or changes to existing) systems and processes which involve the processing of personal data. Consistent assessments are made as to whether proposals meet the statutory criteria to conduct a Data Protection Privacy Impact Assessment (DPIA). DPIAs are conducted by the IG function and approved where effective compliance risk mitigations are confirmed or where the SIRO accepts the risk of not being able to fully mitigate.

Assessments are recorded and a process of review is in place to ensure agreed mitigations remain in place.

## e. Contractual Controls

All Data Processors handling personal data on behalf of the organisation have given assurances about the compliance of their processes; either through procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

Processing of sensitive personal data by the Council's Data Processors is identified and informs a risk rating. Processors identified as undertaking higher risk processing have their practices reviewed or assurances refreshed at periodic intervals dependent on the length of the contract in operation.

**f. Physical Security**

All employees or contractors who have access to the Council's premises where personal data is processed are provided with Identity Cards which validate their entitlement to access. The organisation operates processes which ensure only those individuals who have an entitlement to access premises are able to do so. Access to physical storage holding sensitive personal data is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas of buildings.

The leavers' process, managing activities where employment and access entitlement ends, ensures that ID Cards are returned and securely destroyed or otherwise are disabled.

Data Processors who work within our premises are part of the same controls with the addition that the Council is required through contractual controls to receive leaver data. ID cards for Processors have joint branding to further identify the basis of their entitlement to access premises.

The Council manages visitors to sites through signing-in books, visitor badges and the recording of the details of the Council Officer who takes responsibility for effective management of the visitor whilst on Council premises

CCTV is in operation to secure Council buildings; covering external entrances and some public areas of buildings. Recordings are kept and there is an effective compliant process to support law enforcement and internal security incident investigations.

**g. Security Breach Management**

The organisation maintains a security incident process which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents.

The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale of 72 hours from becoming aware of an incident.

Contracts with Data Processors include appropriate requirements to promptly inform the Council when they become aware of security breaches and to support the Council's investigations and the auctioning of appropriate mitigations.

Incidents are reported to senior leaders and other stakeholders monthly. Actions are consistently taken and lessons learned implemented.

# 2. Technical

## a. Data at Rest

### *i. Use of Hosting Services*

Some personal data is processed externally to the Council's managed environment by Data Processors in data centres under agreed terms and conditions which evidence appropriate security measures.

The Council is aware of hosting arrangements where held or supported outside the European Economic Area (EEA). The DPIA process establishes compliant safeguards and these are communicated to Data Subjects through privacy notices.

The DPIA process ensures that appropriate assurances are received over the security provisions maintained by Processors

### *ii. Firewalls*

Access to the Council's managed environment is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented Information Technology Infrastructure Library (ITIL) compliant change control process which include risk assessments and approvals.

Firewall changes are recorded and reportable to inform risk reviews.

iii. *Administrator Rights*

Enhanced privileges associated with administrator accounts are strictly managed. Administrator activities are logged and auditable to ensure activity can be effectively monitored.

iv. *Access Controls*

Access permissions to personal data held on IT systems are managed through role based permissions. Managers of appropriate seniority inform IT professionals of additions, amendments and discontinuation of individual accounts within permission groups.

Managers are periodically required to confirm that current permissions for which they are the authoriser and details of employees associated with these permissions are accurate.

v. *Password Management*

The organisation requires a mandatory password complexity combination of minimum length and characters, plus a required change of password after 90 days.

vi. *Anti-Malware & Patching*

The organisation has a documented change control process which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

vii. *Disaster Recovery & Business Continuity*

The Council ensures that its systems, whether Council or Supplier managed, have appropriate back-up functionality which is held securely and for a specified period of time to ensure that in the event of an outage, the data can be recovered effectively and utilised to support Council services and the fulfilment of Data Subject rights.

viii. *Disposition*

Digital data deleted from Council systems by authorised users is held in back-up. Deletion from back-up is automated (unless recovered by an administrator for recorded business purposes) and is at this point no longer held by the Council

Paper documents which are not held on formal files are destroyed through secure bins and a weekly transfer to a third party shredding premises via secure tracked transit. Certification of the activity is provided. Reports on volumes destroyed, dates of destruction and volume per individual secure bin are available to the Council.

Destruction of paper records held in formal archive is securely transferred to a shredding facility and the activity is certificated. The destruction of paper records is subject to a process which records the authorisation of a data owner to destroy each record.

**b. Data in Transit**

*i. Secure email*

The Council has access to secure email software for communicating with some third parties where licensing agreements permit this. Sensitive data will be sent using such tools where available. Where software is not available a system of password protecting sensitive data in email attachments is employed which is detailed in policy.

*ii. Secure Websites*

The organisation has access to third party websites which allow for secure upload of personal data. The organisation uses these facilities to fulfil statutory obligations to report personal data to other public authorities.

*iii. Encrypted Hardware*

Devices which store or provide access to personal data are secured by password access. USB data storage devices are automatically encrypted by software on all laptops and desktops before Council data can be copied to them.

Exceptions to this control are reviewed by the Information Governance function and where approved, these are periodically reviewed to ensure risks are being effectively mitigated.

*iv. Hard-Copy Data*

The removal of personal data in hard-copy form is controlled by Council policy which requires employees to take steps to conceal the data and appropriately secure the data during transport.

Certain services are required to formally sign-out case records or record movements on the case management system

The Council requires the use of its paper record archive service to ensure a secure storage, retrieval and destruction system is in place to safeguard non-current records.

These security measures are reviewed annually and approved as accurate and appropriate by the Council's governance process.

| | |
|---|---|
| Date Published | November 2018 |
| Review Due | November 2019 |
| Author | Information Governance Team |
| Version | 1.0 |
| Classification | Official |