Essex County Council

Information Policy Requirements for Contractors

Title	Essex County Council Information Policy Requirements for Contractors
Author/Owner	Information Governance Team
Status	LIVE
Version	1.0
Date Approved	28/06/2018
Review Date	28/06/2019
Security Classification	OFFICIAL

Version	Created/ Reviewed by	Date	Details
1.0	Information Governance	28/06/2018	First published version

Introduction

Where information and personal data are processed by a Contractor on behalf of Essex County Council (ECC), the Council retains responsibility to ensure that it is processed according to the law and to ensure efficient service delivery. To achieve this, the controls within this policy must be in place and the requirements met; managed by Contractor Parties and Staff and monitored by ECC.

This policy is applicable where there is a Contract in place with ECC which includes the accompanying Information Handling Schedule and Data Processing Schedule.

The Contractor must ensure that anyone processing ECC data, defined in the Contract as a Contractor Party or Staff, is aware of these policy requirements.

Data Loss Event Process

Any Data Loss Event or breach of the Information Handling Schedule and/or this policy will be investigated and may result in contractual action.

The Contractor must have processes in place to capture and manage Data Loss Events.

Where regular performance reporting is required by ECC, the Contractor must provide Data Loss Event statistical data. Detailed Data Loss Event evidence must be supplied on demand.

The Contractor must report all Data Loss Events immediately to ECC's Information Governance Team and Procurement Team for formal notification as soon as they are identified and must update ECC on the investigation progress and final resolution as directed.

- In the first instance, an email to notify ECC of the breach is to be sent to the following email addresses, without any personal data or commercially sensitive information:
    - informationgovernanceteam@essex.gov.uk
    - commercial.team@essex.gov.uk
- Following this, ECC will respond via secure email for further detail as required.

Criminal incidents must be reported to law enforcement agencies.

Privacy Management

The Contractor must take appropriate steps to safeguard the privacy of data subjects and only process personal data on behalf of ECC in line with the Data Processing Schedule.

The Contractor must comply with the relevant privacy notice for the service.

Where the Contractor proposes to create a new or amend an existing system/process affecting the processing of personal data, the proposal must be referred to ECC's Information Governance Team for guidance on whether a Data Protection Impact Assessment needs to be undertaken.

Physical Security

Use of ECC Premises:

Where the Contractor is/are based in or utilise ECC's premises, the Contractor must ensure that they comply with ECC ID Cards and Building Security Policy.

The Contractor must supply data on request of those employees who it approves to hold ECC ID Cards. Such data must be sufficient to identify individual employees to manage their card entitlement

.

The Contractor must advise ECC immediately of any individual leaving their organisation so that access to ECC premises can be terminated.

Use of Non-ECC Premises:

The Contractor must ensure that premises (and dedicated areas where ECC data is stored within premises including any Cloud Storage) are protected against unauthorised entry and theft of or damage to ECC data.

Access to building entry keys and keys which secure rooms or storage equipment must be controlled and custody recorded.

The Contractor must regularly change access codes and change relevant codes immediately when an individual's right of access expires.

Data Subject Rights:

The Contractor shall assist the Authority in safeguarding the relevant applicable legal rights of the Data Subject as identified in the privacy notice for the service being delivered.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (Right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- The right to object to Direct Marketing
- Rights related to automated decision making and profiling

If the Contractor receives a Data Subject Right Request they are to immediately notify the Authority's Data Protection Officer.

- In the first instance, an email to notify ECC of the request is to be sent to the following email address, without any personal data:
    - DPO@essex.gov.uk
- Following this, ECC will respond via secure email for further detail as required.

If the Authority contacts the Contractor with a Data Subject Right Request, the Contractor shall provide action on the request within 10 working days of receipt of instruction by the Authority, unless an extension is agreed with the Authority.

Security Classification

ECC complies with the Government Security Classifications Policy: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

All information processed by or on behalf of ECC falls within the category of 'OFFICIAL', with some data falling within the sub section 'OFFICIAL-SENSITIVE'.

Contractors must comply with this classification policy when processing information on behalf of ECC.

Retention and destruction:

ECC data must be retained in line with ECC's Corporate Retention Schedule and destroyed securely with the explicit approval of ECC or by standing agreement with ECC which provides for the Contractor to destroy data once agreed criteria has been met.

Where the supplier destroys data, this activity must be evidenced by recording the criteria for destruction, approval, date and method of the destruction activity and certification of completion, and follow the requirements.

The ECC Retention Schedule is available here:

http://www.essex.gov.uk/Your-Council/Your-Right-Know/Documents/Retention_Schedule.pdf

Where the Contractor has the authority to dispose of ECC data in accordance with the ECC Corporate Retention Schedule or by virtue of any additional agreement, the data must be disposed of by methods appropriate to its security classification.

Destruction processes must ensure that the data is kept secure from disclosure to unauthorised persons until and during destruction, and that the data cannot be reconstituted after the destruction process.

Equipment Security

Devices Accessing ECC Data (such as desktops, laptops, tablets, mobile phones etc.):

- Contractors must ensure that all relevant security solutions are enabled on portable equipment, such as pin codes and password access
- Users must not access ECC data on devices that do not have relevant protective measures in place
- Equipment must be switched off or 'locked' after an appropriate period of inactivity and require a password to re-access
- When stored in office space, laptops must be secured with lock devices or in lockable

storage to prevent theft

- When devices accessing ECC data are used in users' homes, they must be protected from use by any unauthorised persons and must be stored out of sight when not in use to prevent theft
- When laptops are being transported they must not be left unattended, kept out of sight when not being used, and (where available) stored in secure transportation equipment such as a code-lock case
- Any individual for whom the Contractor is responsible (and who accesses ECC data) must return devices to the Contractor when their role requiring access to the ECC data ends, or their role no longer entitles them to such equipment
- Devices accessing ECC data should not be taken outside of the European Economic Area (EEA) unless a) there is a strong business need approved by the Contractor's governance processes and by ECC, and b) there are sufficient security controls in place on the device to allow its use without exposing ECC data to malicious activity or unauthorised disclosure.
- Users must report lost or stolen equipment to the Contractor immediately and where any ECC data is at risk the loss must be handled as Data Loss Event

Asset Management

- A register must be maintained of the physical hardware items (assets) which the Contractor uses to access ECC data. Assets must be uniquely identified, have an identified custodian (who will be accountable for the use and safe keeping of the asset) and have up to date details of versions of relevant anti-malware and encryption solutions installed
    - The register must be promptly updated for new and decommissioned items, change of custodian and change of anti-malware and encryption solutions, so that it remains current
- Paper records must be stored in lockable equipment or dedicated rooms with access to keys or codes managed
    - Such accommodation must include appropriate protection against fire and flood
- Paper filing systems must be well maintained, using clear, logical and consistent referencing and kept in good condition to support identification and retrieval
- When paper records are being transported they must not be left unattended, must be kept out of sight when not being used, and (where available) stored in secure transportation equipment such as a code-lock case
    - Paper records that are being transported must be kept separate from electronic equipment
- Where paper records contain Official-Sensitive ECC data, removing them from storage must be a recorded activity
- Where paper records are in the custody of a third party storage provider, a sub-processor arrangement must be in place as per the Information Handling Schedule. The Contractor must ensure that detailed inventories are maintained to ensure the effective identification and retrieval of individual files and that storage and transfer processes offer appropriate levels of security to the security classification of the data.
- The Contractor must maintain a current and accurate knowledge of the ECC data it holds in all formats, on what systems it resides and the physical locations in which those systems are stored.

- Internal ownership must be established with owners aware of their responsibilities under these requirements.

Removable media

- Removable media refers to USB drives, CDs, DVDs, secure digital cards and devices which permit the storage of data on memory cards, but also refers to hard-copy such as paper files.
- Removable media should only be used where there is a clear business need.
- Where the Contractor allows for the use of removable media, the Contractor must encrypt to an appropriate level any device storing digital ECC data that would cause damage or distress to individuals, or reputational damage to the Contractor or the Authority if it were lost or stolen.
- The Contractor must ensure that the level of security applied to office-located devices is applied to ECC data on removable media being used away from the office.
- Personal data must only be held on removable digital media for transfer purposes and must be securely deleted once copied to its formal storage location.
- The supplier must maintain a removable media policy for the storage of information that:
  - Controls access to, and the use of removal media.
  - Limits the type of media that can be used,
  - Defines user permissions, and the information types that can be stored.
  - Ensures that all clients and hosts automatically scan removable media for malware before first use, and any subsequent data transfer takes place
- Where removable media is to be reused or destroyed, appropriate steps should be taken to ensure that previously stored information will not be accessible.

Email

- The Contractor must ensure that employees are aware of the importance of correctly addressing emails (as with hard-copy mail), to reduce instances of loss of ECC data or it being received by an incorrect recipient.
- Where the Contractor needs to send Official-Sensitive ECC data by email (or post), the Contractor must ensure that employees have been authorised to do so and follow the security classification requirements.
- Where secure email facilities are not available, emails must be sent with the Official-Sensitive ECC data in a password protected attachment, with the recipient informed of the password via an alternative method to email.
- Where the Contractor's employees send ECC data to the incorrect recipient, the Contractor must manage this as a Data Loss Event and ensure the data is recovered. If the data is personal this must be reported to ECC in line with the Data Loss Event Process in order to consider further actions in regards to the data subject and supervisory authority.

Secure Email

- Where the Contractor has access to secure government systems such as PSN (GCSx), CJSM etc and the recipient is able to receive securely, then these facilities must always be used to send Official-Sensitive ECC data.
- Where the Contractor has access to accredited secure email tools then these facilities must always be used to send Official-Sensitive ECC data.

Information Management

Accessibility

- The Supplier must ensure that ECC data held on its systems is maintained in such a way that those who have the rights to access can:
    - Do so promptly;
    - Easily identify and locate information
    - Easily establish the most current and complete version
    - Understand who they may share it with and under what circumstances
    - Easily establish audit trails of services delivered and related authorisations, for use in ECC performance monitoring and internal or external auditing.

Data Quality

The Contractor must provide quality data processes to support effective service delivery and decision making. Quality data has the following characteristics:

- **Accurate:** It must provide a true account of what it is intended to represent to enable informed decisions to be made. Limitations in the level of accuracy must be stated to help appropriate interpretation of resulting information. Maintaining the accuracy of Personal Data is a requirement of Data Protection law
- **Valid:** Data must appropriately reflect what it is intended to measure or report
- **Reliable:** Data must be consistently calculated, recorded, analysed and reported over time in a way that provides a meaningful reflection of the situation to give managers and stakeholders confidence that progress towards targets reflects real changes rather than variations in data collection approaches
- **Timely:** Data must be available frequently and captured promptly enough to be of value
- **Relevant:** Data must be defined/ selected, collected, recorded and analysed with the intended use and audience in mind so that it is fit for purpose and adds value. Consideration should be made towards using anonymisation or psuedonymisation techniques at all times to comply with the Data Minimisation principle in Data Protection law
- **Complete:** Data must be complete and comprehensive to ensure it provides a full picture of a current situation, and caveated where it is incomplete

The Supplier must support regular reviews, sample auditing and provide feedback to achieve and maintain an acceptable standard of data quality.

Acceptable Personal Use

Where information facilities (such as email) can be used to access ECC data, but can also be used for personal purposes, the Contractor must:

- Have a clear policy on what constitutes acceptable personal use,
- Communicate this to all individuals who access ECC data

Where such use is permitted, the Contractor must ensure that activity can be evidenced in the event of ECC data being misused, resulting in an information breach.

Use of ECC's Sharepoint Collaboration Sites

Where the Contractor is granted access to Sharepoint collaboration sites hosted by ECC which allow the sharing and editing of information of mutual interest, the Contractor must ensure that they adhere to the Sharepoint Collaboration Site Guidelines.

Federated Online Messaging (E.g. Microsoft Lync and Skype for Business)

- Where the supplier has federated online messaging functionality with ECC, the facility must not be used for the transfer of Official-Sensitive data and must not be the medium used to communicate and record contract decisions and actions.
- The supplier must evidence appropriate policies and practices in its use of online messaging facilities in order for ECC to approve and maintain federation.

Caldicott principles

The Contractor must observe the Caldicott Principles when processing health and/or social care data, which are set out below:

- **1. Justify the purpose(s)** - Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
- **2. Don't use personal confidential data unless it is absolutely necessary** - Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **3. Use the minimum necessary personal confidential data** - Where use of personal confidential data is considered to be essential, the inclusion of each discrete item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function.
- **4. Access to personal confidential data should be on a strict need-to-know basis** - Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for

several purposes.

- **5. Everyone with access to personal confidential data should be aware of their responsibilities** - Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical employees — are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **6. Comply with the law** - Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
- **7. The duty to share information can be as important as the duty to protect patient confidentiality** - Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Protective Measures

ECC requires its Contractors to have relevant technical and organisational measures (Protective Measures) in place to protect ECC Data. As well as the supplier of a solution/service, this also applies to any sub-contractors/sub-processors the Contractors uses (or intends to use) to provide the solution/service – any that will access, process, store or communicate information, or provide IT infrastructure components. It's the Contractor's responsibility to check that all these parties have relevant Protective Measures in place.

ECC recommends that Contractors follow best practice guidance and have in place Protective Measures in line with the following:

- National Cyber Security Centre (NCSC)'s 10 Steps To Cyber Security
- The Information Commissioner's Office Practical guide to IT Security
- NCSC's Cyber Essentials

Where certification or accreditation is held by the Contractor that demonstrates the Protective Measures that are in place (such as a Cyber Essentials Certificate), this should be provided to ECC by emailing informationgovernanceteam@essex.gov.uk

Appendix A – SharePoint Collaboration Site Guidelines

Where the Supplier is granted access to SharePoint sites hosted by ECC which allow the sharing of and collaboration on information of mutual interest, the Supplier must ensure that:

- There is a register maintained of employees who have access to sites, and that the access is at all times necessary and therefore valid and available for auditing by ECC.
- Where employees leave the Supplier's organisation, or when they change to a role which no longer requires access or when access credentials have been compromised, the Supplier must inform the relevant ECC SharePoint Site Manager to allow accounts and permissions to be managed accordingly
- Those with rights to add or edit documents must comply with the ECC Site Owner's requirements over assigning document metadata, titling conventions and correct document library storage
- Copies of documents containing ECC data available on the sites are not stored outside of the site or shared/ disclosed beyond the permissions group of the site without the permission of the Site Owner.
- Where a site is accessible by a number of Suppliers and Partners, any information which a Supplier does not wish to be available to anyone other than ECC and its own employees must be stored in a document library for the appropriate audience, provided by ECC.
- Its employees are aware that all information on the site is accessible to ECC and is information held by ECC for the purposes of the Freedom of Information Act (2000), with the Supplier offered the opportunity to present prejudice and public interest cases prior to disclosure.
- Where the Supplier is a Public Authority under Schedule 1 of the Freedom of Information Act (2000), its employees must be aware that disclosure of any ECC data stored on a site in response to requests for information must be referred to ECC for clarification on whether the data is held for the purposes of the Act, and if so, for consideration of valid exemptions.

Appendix B - ECC ID Cards and Building Security Policy

- You must not allow anyone to follow you through a security door (tailgating) without clearly displaying a valid ID Card.
- You must carry your ECC ID Card or Visitor pass and display it at all times when in ECC buildings, or to prove to a member of the public or staff of another organisation that you are representing ECC on official business. Otherwise, when outside of ECC premises you should keep your pass hidden to ensure personal security.
- You must not share your ECC ID Card with anyone, or share door codes or keys with unauthorised people.
- If you find a lost ECC ID Card, you must hand it in to the nearest reception or security office.
- If you lose your pass or it is stolen, you must report it to Mitie Security.
- All leavers must hand their pass to their line-manager as part of the leavers' process.
- You must supervise all visitors that you allow into a secure work area at all times until they leave.
- You must ensure door codes and security alarms are changed regularly.
- All employees must ensure offices are secure if they are the last person to leave at the end of the working day.
- Mitie security must perform regular checks of staff compliance with this policy.
- All employees/ agency workers/ consultants/ elected members must assist Mitie Security with checks of compliance with this policy.
- Any ID Card which provides access to ECC buildings, or visibly identifies a person as being employed by ECC (or by an employer in partnership or under contract to ECC), or visibly identifies that a person has been approved by ECC to carry out a service, must be provided and recorded by Mitie.
- If you are a line manager or are approving requests on behalf of partner or supplier staff, you must ensure that any access rights you approve on staff application forms are valid.
- The Information Governance Team must maintain a list of partners and suppliers who are approved to have ECC ID Cards.
- If you are a Commissioner of an external service provider or are managing the relationship with a partner who is authorised to use ECC ID Cards, you must ensure the third party complies with this policy and the Procedure for Managing ID Cards.