Essex County Council

Information Policy Booklet

Title	Information Policy Booklet
Author/Owner	Information Governance Team
Status	Final
Version	1.0
Last Review Date:	February 2023
Security Classification	Official

Contents

1. Introduction to the policies

The policies in this booklet set out how those working for, or on behalf of, ECC are required to handle the information and equipment they use or to which they are able to access in performing their role.

The aim of the policies is to help people know what is expected and required of them.

If you have any queries about this policy and how to apply it, please contact the Information Governance team (IG), IGTeam@essex.gov.uk, 033301 39824.

2. Data Protection laws

All organisations in the UK have to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA18), both of which are enforced in the UK by the Information Commissioner's Office (ICO). The ICO has a number of powers including the power to fine organisations up to the equivalent of €20m or 4% of global turnover (whichever is higher) for Data Protection breaches. Our policies are in place to minimise the potential of such actions against ECC.

All employees and people handling ECC data are required to comply with the policies in this booklet. They will help you protect the individuals whose personal data is being processed by the Local Authority.

What is Personal Data?

There are two categories of data.

- Personal Data – this only includes information relating to natural persons who:
  - can be identified or who are identifiable, directly from the information in question; or
  - who can be indirectly identified from that information in combination with other information.
- Special Categories of Data -
  - personal data revealing racial or ethnic origin;
  - personal data revealing political opinions;
  - personal data revealing religious or philosophical beliefs;
  - personal data revealing trade union membership;
  - genetic data;
  - biometric data (where used for identification purposes);
  - data concerning health;
  - data concerning a person's sex life; and
  - data concerning a person's sexual orientation.

It is important to know if you are dealing with special category data the rules are slightly different and a breach involving special category data is generally considered to be more serious.

What the rules are

There are seven UK GDPR principles that must be followed:

1. Use it lawfully, fairly and transparently
2. Use it only for the purpose it was collected
3. Use the minimum amount of data necessary for the purpose
4. Ensure it is accurate
5. Do not keep it longer than needed
6. Keep it secure
7. Retain records of decisions made to demonstrate accountability

The UK GDPR gives individuals (whether these be customers, or members of staff) controls. These include the following rights:

1. The right to be informed how their data is used
2. The right to access copies of their data
3. The right to rectification of data when it is incorrect
4. The right to be forgotten (although this is rarely possible in health or social care)
5. The right to restrict processing
6. The right to move electronic information to another organisation
7. The right to object to processing of their data
8. Rights in relation to automated decision making and profiling.

Law Enforcement Processing, both civil and criminal, is not covered by the UK GDPR, but is included in Part 3 of the Data Protection Act 2018 in Part 3. If you are processing data for law enforcement purposes you will need to be aware of the wider legal framework, in particular Part 2 of the Act, which covers aspects of the UK GDPR that allow for national exemptions in specific instances.

ECC is a competent authority for the purposes of Part 3 of the Act as we process personal data for law enforcement purposes, for example our Trading Standards Team, Child and Adult Protection Teams, Traffic Enforcement Team, Coroners, Youth Offending Service etc.

Further detailed information around Law Enforcement processing can be found in our Law Enforcement processing guidance.

a. Lawful basis

You must have a lawful basis for processing personal data and most lawful bases require it to be necessary for a specific purpose:

- **Consent**, the GDPR sets a high standard for consent. But you often will not need consent. If consent is difficult, look for a different lawful basis.
    - Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
    - Consent is “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he

or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

- Processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a **legal obligation** to which the controller is subject.
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

These are the lawful bases for personal data, special category data needs more protection because of the sensitivity. Guidance on these can be found on the ICO website.

b. Privacy Notices

Under the Data Protection Legislation whenever we collect personal information about an individual, we must tell them why we are collecting it to assure them that their information is collected and used fairly and in a transparent manner.

ECC privacy notices are published on the internet. If you have provided details to be included within the notice it must be reviewed annually.

A privacy notice is required to tell people the following and we must ensure we are complying with this requirement:

- The identity and contact details of the organisation, its representative, and its Data Protection Officer.
- The purpose for the organisation to process an individual's personal data and its legal basis.
- The legitimate interests of the organisation (or third party, where applicable).
- Any recipient or categories of recipients of an individual's data.
- The details regarding any transfer of personal data to a country outside of the European Economic Area and the safeguards taken.
- The retention period or criteria used to determine the retention period of the data.
- The existence of each data subject's rights.
- The right to withdraw consent at any time (where relevant).
- The right to lodge a complaint with a supervisory authority.
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.

- The existence of an automated decision-making system, including profiling, and information about how this system has been set up, the significance, and the consequences.

A sample privacy notice for surveys and forms:

Essex County Council (ECC) is the controller of the personal information you provide to us. The personal information collected on this form will be used by ECC for the administration of school transport under the Education Act 1996. This information will only be shared with your relevant school and selected transport operator for the purposes of providing school transport and applying the policy. If we suspect fraud or crime is being committed, we may also share your information with the police and other fraud investigation organisations where the law requires us to do so. For more detail on how your personal information is used and your right, please visit www.essex.gov.uk/privacy.

c. Surveillance

This section explains how to manage surveillance tools such as CCTV systems, Drones, Automated Number Plate Recognition (ANPR), Dash Camera and Body Worn Cameras (BWC); and the use of personal data of employees or representatives for monitoring purposes within the law.

ECC services may use surveillance tools for a variety of purposes, for example:

- The prevention and detection of crime and fraud
- To carry out inspections
- For health and safety purposes

Where we process personal information and in circumstances where the data subject may not be aware (invisible processing) we must ensure that we do so lawfully.

Our use of surveillance must be proportionate, necessary, legitimate and justifiable.

Personal data should only be processed for a specific purpose and must not be excessive for meeting that purpose. ECC must consider alternative methods of meeting the aims and decide if the proposed monitoring tool is the most appropriate method to achieve the aim.

There must be a pressing need for the use of a surveillance system to be appropriate. Any surveillance equipment must be impact assessed to ensure we have documented the necessity and legitimacy for the intended use.

When making automated decisions on individuals' personal data, every effort must be made to ensure the data has been verified as accurate.

The European Data Protection Board (EDPB) guidance makes clear that any surveillance must have signage, and it should be layered. This must be clearly visible where surveillance is in operation and it should be noticeable before an individual has entered the space in which the surveillance is taking place. It must contain:

- The name of the Data Controller
- The name of the Data Protection Officer
- The purpose of the processing
- Data Subjects rights
- How to access the full privacy notice (QR code or web address)

Our privacy notices must ensure that where monitoring is used individuals are aware of their rights and how to exercise them. Access to any recordings must be restricted to protect the confidentiality, integrity and availability of the data.

To comply members of staff must follow the below:

- All use of CCTV recording, Drones, ANPR, or Body Worn Cameras must be approved before it becomes operational.
- All types of surveillance activity are subject to a Data Protection Impact Assessment (DPIA).
- The approval of surveillance operations must consider the effect on individuals and their privacy.
- There must be transparency and appropriate signage in the use of surveillance tools.
- There must be clear responsibility and accountability for all surveillance activities, including who can gain access to view live images and recordings, and for what purpose such access is granted.
- The disclosure of images and information should only take place when it is necessary for a stated purpose or for law enforcement purposes. All instances of access must be approved in line with the Surveillance and RIPA Policy.
- Images and information must have a defined retention period and be deleted once their purposes have been discharged.
- Overwriting surveillance recordings after 31 days. This retention period is arrived at by analysing the typical length of time after a recording is made that there is a legitimate need to refer to it within our stated purposes.
- In managing a surveillance system, ECC must consider any approved standards or certification schemes relevant to maintaining compliance.
- All surveillance equipment must be subject to appropriate technical security measures, including the ability to redact third party images, restricting access to rooms where surveillance footage can be viewed, and recordings can be accessed. Logging entry to such rooms. Password protecting systems which permit entry to recordings. Ensuring the network on which the recordings are stored is secure and robust.
- Must ensure that the images are of good quality and are date and time stamped.
- Any use of surveillance to search for or follow a person or to use surveillance for a law enforcement operation is likely to be “directed surveillance” which needs to be authorised under the Regulation of Investigatory Powers Act 2000.
- Any dataset which is matched against data recognised by surveillance equipment must be kept up to date.
- Regular reviews to ensure its use remains justified must be undertaken for the use of a system to be appropriate. This should include a published contact

point for access to information and complaints which is clearly visible on signage and available on the ECC Internet.

- These provisions must be communicated to all staff (and suppliers) who need to comply with them. The Surveillance Guidance provides a clear scope and treatment of surveillance issues and is supported by Subject Access Request forms.
- All requests must be properly authorised unless they are part of a response to an emergency, even if they are made by the police. You must refer any such requests to the monitoring officer.

d. Monitoring of emails and electronic communications

Monitoring of employees is only permitted if it is lawful, necessary to achieve a lawful business purpose and if it is approved by IG.

If you intend to monitor employees, the following will apply:

- Before monitoring can begin, a line manager must discuss informally with IG.
- Where an employee is suspected of non-criminal breaches of policy, they must be given advice and then be informed that monitoring will take place if the activity continues.
- Where an employee is suspected of criminal activity, monitoring must be considered under the Regulation of Investigatory Powers Act (RIPA).
- If an assessment is approved, then IG or Internal Audit will arrange for the monitoring to be done and the results provided to the line manager.
- If you know or suspect that someone else is monitoring staff without permission you must raise a Security Incident.
- ECC must not use information we collect through monitoring for any other purpose than the original agreed purpose.

3. Security of personal information

a. Security Incidents

A security incident is a confirmed or potential failure of the controls we put in place to prevent the risks to our information from occurring. These could range from failure to follow a policy resulting in inadequate data sharing or a technical error resulting in information being exposed or lost. The full list of what we consider to be a security incident is in the Security incident procedure.

A security incident could also be a breach of the UK GDPR. If this is the case, we may be required to report the breach to the ICO and could be subject to a fine.

It is important that any actual or potential security incident is reported immediately, to ensure we can act quickly to take to reduce the risk of damage and/or distress caused to any individual.

b. Cyber Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies.

A cyber attack is any attempt to gain unauthorised access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

For more information about specific policy areas to be adhered to by all employees to safeguard against cyber attacks go to:

- Section 3c – Network Security including passwords
- Section 4a – Use of emails

More information can also be found on the IG Cyber security playlist on MyLearning.

c. Network security

You must not do anything that would compromise the security of ECC's network. This could include:

- Using apps or cloud system not approved by Technology Services.
- Knowingly downloading or spreading any computer virus or other program that is harmful to normal computer operations.
- Disabling or changing standard security settings such as anti-virus protection or encryption.

Any user of an ECC system must:

- Set strong passwords/PINs, see guidance from NCSC.
    - Weak passwords can be easily cracked. The longer it is, the stronger it is and the harder it becomes to hack. Make yours strong by using a sequence of three random words.
    - It must be at least nine characters long and where possible must contain at least one character from three of the following groups:
        - Uppercase character (e.g. A-Z)
        - Lowercase character (e.g. a-z)
        - Numbers (i.e. 0-9)
        - Special Characters (!£$%^&*<>?@#|~)
- If you believe someone else may know any of your passwords, change at the earliest opportunity and always change when prompted.
- Do not set to 'never expire', or store on applications or websites.
- Do not use the same password for accessing more than one business website or application.

- Never use a work password for accessing personal websites or applications.
- Do not use generic logins (multiple users sharing a password) where possible.
- Suppliers and partners must not be given access to the ECC network unless that is approved by IG.
- You must ensure the starters and leavers process is followed including for maternity leave and long-term absence as accounts will be suspended after 45 days of inactivity and deleted after 90 days of inactivity.
- Line managers must ensure the leavers process is followed for all staff leaving ECC employment to ensure access to ECC data is revoked.

d. Protecting information assets and devices including mobile and flexible working

When working with ECC information you have a responsibility to ensure its security. All information must remain in your control wherever you are working. When you are physically transporting ECC data outside of ECC premises, whether on paper or on portable storage including CDs, DVDs, USB memory stick etc.. You must take steps to keep it secure to prevent any accidental loss (e.g. papers or removable media accidentally falling out of bags), or theft (by exposing papers or equipment and not securing them properly).

When outside the office, items must be kept hidden from view to others:

- You must not leave Official-Sensitive data or devices unattended in a vehicle for longer than 10 minutes and, you must:
    i. Make sure the item and any bag are out of sight of passers by
    ii. Ensure that the vehicle is not left in a place which is known to present a high risk of thefts.
- You must take appropriate steps to prevent accidental loss, unauthorised use and theft.
- You must ensure that only authorised users can access ECC information wherever it is stored.
    i. You must not allow family members or friends to use ECC IT equipment or have access to ECC information even if you are present.
    ii. You must ensure that if you access ECC data on your own device then that information is locked from other users.
- You must make sure that when IT equipment and hard-copy information is not in use that it is stored securely out of sight. Review the Home Working intranet pages and Policy, if you believe you may qualify as a home worker.
- If you use browser/apps to access ECC information, you must not save your password. This introduces the risk of someone who can gain access to your device, also getting easy access to the ECC data. Do not approve any offer from your devices to save any ECC password.
- Do not take information or devices abroad unless approved by your line manager after consulting Information Governance team or any specific

guidance produced by Information Governance. Permission should not be given to take equipment or data to a location which places it at risk.

- If you are taking shared Official-Sensitive information out of the office in paper form or removable media, this must be recorded. This is to make sure that ECC knows who has custody of important information at all times.
- Managers should ensure that employees' have access to systems which allow you to 'sign-out' or record what information you are taking custody of, when returned, why and under whose authority.
- Where you hold sensitive conversations relating to ECC information, you must make sure they are only audible by an appropriate audience.
- If you overhear or are exposed to information which you should not have access to, you must alert the information custodian to the fact that they are not managing the information appropriately.
- When connecting to home Wi-Fi router you must ensure it is secured to encryption level WPA/WPA 2 for security, and the traffic you send over it is encrypted. Please use the link https://ico.org.uk/for-the-public/online/wifi-security/ which details how you can check your Wi-Fi status and update this.
- When connecting to public Wi-Fi such as coffee shops or hotel Wi-Fi, Windows asks if it is a 'public or private' network, you must select 'public'. A public network has the discovery settings turned off and doesn't allow file and printer sharing. Your device will then use the network to connect though to the ECC Network via direct access which uses a secure tunnel, providing a secure connection.
- Criminal Justice Secure email (CJSM) must not be sent when connected to public Wi-Fi such as coffee shops or hotels. ECC is required to comply with this as a condition of accessing CJSM.
- When you need to send CJSM emails, you must always check what network you are connected to first, to ensure it is not a public Wi-Fi network. If it is, disconnect and connect to a secure network instead.

e. Physical security measures

Physical security measures must be applied when conducting ECC business, to ensure the security of personnel, buildings and visitors;

- You must carry your ECC ID card or visitors pass when in ECC buildings and hide from view when not conducting ECC business to ensure personal security. Visitor or third-party ID cards are available from MITIE security.
- Never tailgate through doors, always show your security pass.
- Never share your ID card or door codes/keys with unauthorised people.
- Lost/found ID cards must be reported to MITIE security.
- All leavers must return their ID cards to their line manager.
- Ensure door codes and security alarms are regularly changed.
- Supervise all visitors that you allow into a secure work area.
- If you are the last to leave your place of work, ensure offices are secure.

f. Disposing of personal data

Paper records must be destroyed by use of:

Sensitive Waste Service: where you must follow the process managed by Mitie, or
Archive Storage: where information is in the custody of Mitie's Records Management Service, it must be destroyed by the secure shredding service operated by the approved archive storage contractor.
Removable digital media (such as USB memory sticks and external hard-drives, old Central Processing Units (CPUs), Floppy Disks, CDs, DVDs, Video tapes, Audio cassettes; any medium on which digital information can be stored) must be destroyed by the process managed by Technology Services.

Information stored on ECC's **systems** (such as emails and electronic documents, spreadsheets, presentations etc) must be:

- **Emails**: deleted from inbox/sub-folders/archive, and then from deleted items.
- **Files**: deleted from ECC systems, Teams and OneDrive.

g. Security Classification

We have legal obligations to protect the information we process at ECC. One way we do this is by classifying the information we handle, as either Official or Official-Sensitive. This is to ensure information is handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack.
All staff must be trained to understand they are responsible for securely handling any information, in line with local business processes.
Read the Security Classification Guidance to ensure you are correctly handling information.

4. Moving information around safely

This section covers your responsibilities when using communication tools such as;

- email,
- instant messaging,
- Microsoft Teams and other parts of Office 365
- mobile devices and telephony including voicemail/video recording,
- online surveys and
- printing, posting, faxing and scanning.

Remember:

- All information gathered via these communication means including audio and video recordings must be managed as potential ECC records and in line with all aspects of this policies document.
    i. Ensure that it is stored securely and not shared with anyone who is not entitled to access the recording.
    ii. When the recording is no longer required you must destroy/delete securely in accordance with the Records Retention Schedule and the sensitive waste requirements.
    iii. They are subject to Subject Access Requests, Freedom of Information Act and Environmental Information Regulations.

- Review the Classification section to help identify the security classification of your documents and the appropriate handling advice.
- When considering using voice and video recording facilities such as voicemail, OneNote, voice recorders, cameras, Dictaphones, mobile phones and tablets you need to ensure you have a legitimate need to record as part of the council's role as a public authority, or that you have consent from everybody present before recording begins. Failure to gain consent could result in a breach of the Data Protection Legislation.
- You must not leave sensitive information unattended when you print, photocopy or fax. We have a duty to ensure that sensitive information is only accessible to those who are authorised to see it.

a. Use of Email

Emails can be and often are formal business records. This means they should be managed as records.

- Your email system must not be used for filing business information, this information should be in a shared environment (with appropriate folder security if Official-Sensitive) or system. The retention policy relating to Outlook items is as follows:
    - Voicemail: 30 days
    - Conversation History (instant messages): 90 days
    - Leavers: 30 days
    - Junk email: 30 days

- When carrying out ECC business you must only use an **ECC provided email** for ECC business. Use of personal email addresses to send and receive ECC data is not permitted.
- You must arrange for cover during any absence by giving delegate rights to at least two other people (including your line manager) to allow access to the parts of your mailbox that contain business information, including inbox, subfolders, sent items and calendar. Delegates access must only be used for business purposes and line managers must ensure they can access the email of everyone they manage.
- If you are the owner of a team or distribution list or group mailbox you must ensure you annually review the recipients/members. Ensuring the right people have access and that if you leave ECC or change role, another owner is in place.
- You must follow the Dealing with Nuisance or Malicious Email guidance when managing emails which you suspect contains viruses/malware or is spam or phishing. If you suspect that there is a virus in an email, you must immediately delete it as a precautionary measure without forwarding the email on to anybody else. Our security software usually prevents any malicious attacks coming through to mailboxes.
- Always check that the recipients of e-mail messages are correct so that potentially Official-Sensitive information is not accidently provided to unauthorised people.

- You must not setup an auto-forward rule which re-directs all your emails from your ECC email account to a non-ECC email account.
- You must not email any Official-Sensitive information to your personal home email address; or a printing service other than one procured centrally via ECC.
- You must not put personal names in the subject line of emails. If you receive an email containing sensitive personal information in the subject line, you must remove it before forwarding/replying.
- You must not access CJSM email from outside the UK. If you do have a requirement to access CJSM from outside of the UK contact the Information Governance team for advice. IG with inform the CJSM Helpdesk before granting approvals.

b. Instant messaging/telephony (excluding O365)

Although instant messaging is typically used for informal conversation, the text of the discussion is retained and is "held" by ECC for the purposes of information legislation making it potentially disclosable unless deleted.

- Information sharing through instant messages with partners and suppliers must be done in accordance with the relevant contract or sharing agreements to ensure ECC complies with the law when sharing personal data, and that ECC's sensitive data is handled appropriately.
- You must not share **Official-Sensitive** information through instant messenger to anyone external to the ECC network. Instant messenger does not offer the high levels of security required for data of this sensitivity.

c. Mobile Devices

By 'mobile device' we mean any tablet or phone.

- Employees accessing ECC information through an ECC-provided mobile device or their own personal device must agree to and comply with the requirements of the "ECC Smart Device" guidance. This will ensure that ECC information is handled securely, where ECC cannot fully control what a user can do with that data through technical means.
- Photographs or videos which include images of people are regulated by information law. This means that if you take a photo on a mobile device you must:
    - Ensure that the photograph is saved to an ECC system or network.
    - Ensure that the photograph is removed from the device and not backed up elsewhere (e.g. in iCloud or google photos).

d. Printing and Scanning

- You must check when you finish scanning that the files have been scanned correctly, to the correct location and that you have removed scanned documents from the scanner. Check that the scanned version of your document is an accurate copy of the original before disposing or filing of the original.
- You must not leave scanners unattended whilst printing or scanning large quantities of documents. The documents could be accessed by someone who is unauthorised to view them. Stay with the MFD until the printing or scanning is complete (evacuating offices in an emergency is an accepted reason for leaving documents, but they must be recovered once employees are asked to return to the office).

- If you are printing Official-Sensitive information, you must not email information to a personal email address, or an online print service. These methods can put the security of the information at risk. For 'Official' information the risks are accepted, but for 'Official-Sensitive' they are not.

e. Posting and Hybrid Mail

- You must carefully consider the risks of posting Official-Sensitive information and put appropriate controls in place to protect the information. This is to evidence delivery in cases where this is necessary.
- When posting ECC documents, you must use the Hybrid Mail system (Dataforge).
- Confirm the name or job title of the recipient, department and full address.
- When posting ECC information, the envelope/package and the letter content must include an appropriate return postal address**.**
- When posting electronic media which store data, you must password protect the device, send the password to the recipient by another means and then confirm they have received it.

f. Internal Post

- If using envelopes, ensure all previous location information is fully crossed out to ensure it arrives at the correct location.
- Do not put any information in the internal post that is not in an envelope.

g. Safe Haven Fax Process

Fax machines must only be used when necessary. When sending personal identifiable information always:

- Ensure the recipient knows the fax is being sent.
- Ensure the fax will be collected at the other end.
- Send the front sheet through first.
- Check that it has been received by the correct recipient.
- Add the rest of the document to the fax.
- Press the redial button.
- Don't walk away while transmitting.
- Wait for the original to process and remove it from the fax machine.
- Wait for confirmation of successful transmission.
- Consider whether it is appropriate to fax to another colleague if they are not there to receive it.
- Use only the minimum information and anonymise where possible.

h. Information Sharing

Data Protection Legislation is not a barrier for sharing information. Under the right circumstances and for the right reasons, data sharing can play a crucial role in providing a better, more efficient service. The ICO has a Data Sharing Code of Practice along with Data sharing checklists to assist when making the decision to share.

Data Processing has a legal duty to make clear to third parties how we expect them to process information on our behalf, and a duty to provide assurance to individuals and partners that this activity is within the law. An effective contractual control must be in place for information we provide or transfer to third parties to deliver services on our behalf. A data processing schedule should be included in a contract to detail the data processing.

If the contract does not provide enough detail about specific information sharing you must ensure an Information Sharing Protocol is in place with our partners and suppliers:

- Share personal information between partner organisations under transparent and legally sound Information Sharing Protocols (ISPs).
- Ensure the sharing is regularly assessed against legal requirements to provide assurance to involved partners that information sharing remains within the law. Where ECC is the lead organisation in an information sharing arrangement, it is responsible for conducting reviews of ISPs. *N.B. Reviews must be set to no longer than three years from the time the ISP is approved by all partners.*
- Ensure all sharing of personal information is done lawfully and all legal bases have been documented for all partners. The legal basis for a partner organisation may be different to ECC's. The ISP can be used when sharing arrangements are required with any external organisation/s.
- Final versions of all ISPs where ECC is a signatory must be sent to IGTeam@essex.gov.uk with any email approvals for audit purposes.

ECC must maintain an appropriate level of compliance with the requirements of the Data Security and Protection Toolkit (DSPT). The DSPT is a key means of assuring partners that ECC is a trusted authority and has mature compliant processes in place to safeguard our information and those who share their information with us. Maintaining compliance is a key requirement to retain our entitlement to shared systems and networks with partners.

ECC must have effective controls in place where suppliers are given access to ECC information. One of the following must be in place with the suppler if ECC's network or systems access is required:

- Where a contract is in place including the ECC Information Policy Requirements for Contractors then enough assurance is in place
- Where a contract is in place but was agreed before the ECC Information Policy Requirements for Suppliers was included (pre-Feb 2016), then Appendix D of the Policy Requirements document must be signed by an appropriately senior employee of the contractor. Please use the hyperlink above.
- For new starters where there is no contract in place between ECC and the third party/company as the applicant does not work for a company, you will need to complete a Non-Disclosure Agreement as part of the 'Starters Process'. Applies to self-employed contractors, volunteers etc.

5. Good housekeeping

You must not do anything that would compromise the security of ECC's information by using apps or cloud-based systems that have not been approved by Technology Services. You must not allow anyone access to your ECC IT account. All activity on your ECC IT account is assumed to be yours. Logs of activity are maintained; you are accountable for any wrongdoing through your account.

a. Clear Desk Clear Screen

- ECC hard-copy (paper) information must be locked away at the end of each working day or when the office is unoccupied.
- IT equipment which stores personal information (such as laptops, phones, tablets and removable storage media) must be secured in locked pedestals or cabinets at the end of each working day or when the office is unoccupied.
- Whenever you leave your device or have a visitor who is not authorised to view the information you are working on, you must always lock the screen or sign out of the internet browser. It prevents someone from reading confidential information left open on the screen.

b. Team Moves and Building Closures

All office moves/building closures must go to Mitie helpdesk (ecc.helpdesk@mitie.com) for approval by Essex Property and Facilities. Once approved a move co-ordinator must be appointed by the service and will be responsible for the following:

- Employees have clear instruction on what information to pack-up, archive or destroy.
- Enough time is available to employees to do these tasks ahead of the move.
- ECC information and information storage equipment must not be left in the office space after a move date, unless agreed with Mitie.
- A check of the vacated office or whole building must be made by the Team Manager ahead of the closure sign-off.

c. Data Quality

Data is essential in national and local government, and almost all our core activities require the use of data. Information is the product of data that is created by processing, manipulating and organising data to answer questions that adds to the knowledge of the Council. This knowledge (also called intelligence) often involves interpreting the information and adding relevant context that clarifies the insights the information contains.

When handling ECC information it should be sufficiently accurate for the intended purpose and in line with the standards for anonymisation and pseudonymisation where required.

All employees must ensure that they collect, manage and use information appropriately and effectively by:

- Information is provided in a way that is responsive to customer needs.
- Enough quality to enable effective decision making.
- Anonymising or pseudonymising in line current standards.

- Risk assessing the possibility of re-identification to protect individuals' privacy rights.
- Applying data quality standards to business as usual activity, projects and performance data.
- Regularly review Data Quality guidance available.
- Take proactive steps to minimise errors at point of data collection.
- Report any inconsistencies or issues to their line manager.
- Manage these policy requirements alongside the service specific responsibilities that employees may hold through job roles, or through service level agreements.
- Have appropriate controls in place when publishing data.
- Ensure business continuity arrangements are in place for data set availability.
- Personal information is deleted once its purpose has been fulfilled.
- If storing information for longer than six months after first-use, employees must secure on-going consent from customers, and agreement from IG.

6. Making Information Accessible

When working with ECC data you must ensure it is accessible.

Accessing information

- You must only access ECC systems for a legitimate business need and must not look at your own personal or family and friends' records.
- You must document business activities in accordance with local service procedures.
- You must store all information in the format and medium best suited to its use in line with service procedures.
- You must ensure that you give access to a delegate for business continuity purposes.
- When saving resources (documents, videos, forms, stream, and power automate etc) you must ensure you move Official-Sensitive information to the appropriate Teams or System for Business Continuity purposes. Resources are saved to OneDrive by default, and you must use this as a draft area and move as soon as possible.
- You must review all MS Teams sites of which you are the owner at least twice a year to ensure that:
    - all MS Teams sites have two owners to manage access to ECC information.
    - Teams automatically expire after one year; owners must ensure they review and act if the site is still required.
    - Review the access you have provided to information.
- Regularly review information to make best use of the available storage space, both physical and electronic.
- Follow the Managing Electronic Records Guidance when storing information.

- Ensure that the facilities available for storing and managing information meet the requirements of the Records Lifecycle & Systems Procedure and Metadata Guidance.
- Help to make information more accessible to others by making full use of facilities to add metadata to documents or records within systems, in line with the Metadata Guidance.

7. Designing our policies and activities well

a. Data Protection Impact Assessments (DPIA)

A DPIA is a review you must carry out to help you identify and minimise the data protection risks of a project or a data flow. It is legal obligation under the UK GDPR, and when done properly helps assess and demonstrate how we comply with all our data protection obligations.

If you are managing any activity or proposed new activity such as creating a new process, amending an existing process, purchasing a service or conducting a procurement exercise which involves the use of personal data. You must contact IG to begin the DPIA process.

IG will assist you with mitigating some of these risks by supporting you to undertake an impact assessment on what you are looking to do. This assessment will cover information security, data quality and privacy as well as other governing information legislation.

If you are managing an initiative or activity which requires a DPIA, you must begin the process as early in the project as possible.

Where the activity involves is high risk processing IG will seek approval from the Data Protection Officer to approve.

More guidance and a link to the DPIA form can be found on this link.

b. Payment Card

Any organisation processing payment card details must ensure they are compliant with the Payment Card Industry Data Security Standard (PCI DSS). As part of the compliance you must ensure staff are aware of their responsibilities when handling financial data provided to us when customers purchase goods or services. Anyone processing card payments on behalf of ECC must only do so using the following methods/ equipment:

Where the customer is present (face-to-face)

- Chip and PIN
- PDQ Terminal
- Till system

Where the customer is not present (payment over the telephone)

- CapitaPay 360

- PDQ Terminal

Follow the Payment Card Security Procedures:

- Securely retain or destroy the authorised receipts generated by the system or PDQ terminal in line with the council Retention Schedule.
- Ensure all refunds are made to the same card as the payment was taken on and not made to any other card or by any other method.
- Delete any emails where the customer has enclosed their payment details.
- Never take screen shots, photographs, videos or voice record any customer payment details.
- Report any suspected breach of security or fraudulent activity.
- Follow the procedure if equipment failure means you need to use a manual method of card payment.
- Managers must ensure that only authorised personnel may be given access to the chip and pin terminal or enter an area where payments are taken by telephone or in person.
- Financial controllers must ensure access to payment systems and payment card information is restricted to those individuals who are involved within the payment process.
- Complete ECC's annual PCI DSS compliance eLearning module.
- Never use email to send payment card details.
- Do not transmit electronically or forward by hard copy any customer payment details.
- Where payments are being processed, you must not keep any personal bags of any description on your desk and not use cameras, mobile phones with cameras etc. whilst processing transactions.

Extra Requirements for PDQ Terminals:

- Verify the identity of any third-party person claiming to be repair or maintenance personnel, prior to granting them access to modify the devices.
- Be aware of any suspicious behaviour around the devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behaviour and indications of device tampering to appropriate personnel (for example, to a manager).
- Do not install, replace or return devices without verification

c. Violent People Markers

When managing information about people who may pose a health and safety risk to ECC staff and others, you must consider the need for a marker to warn people who may come in contact with that person. This is captured in the Health & Safety People Warning Marker Procedure.

Thing to remember:

- If the marker is approved, the individual and the victim of any violent action will normally need to be informed.
- When informing the individual of the marker in place they need to be advised of the ECC appeals process.
- All markers need to have a review to determine whether it should remain in place or removed.

d. Online Surveys

- When designing an online survey to get opinions that will help ECC develop and target services, you must carefully select what questions you wish to ask to deliver the necessary outcome.
- When drafting questions for the survey, challenge yourself over whether the questions you are asking will result in insight/data will meet the objectives of the project/consultation. This will then inform a decision on whether it is proportionate to ask the question.
- If you need to collect personal or sensitive personal information, you should only do so if you have an appropriate reason and you must make it clear in the survey that the information is optional.
- If you are collecting personal or sensitive personal information, the survey must include a privacy notice. The privacy notice is our means of telling people what those purposes are. Please see the privacy notice section.
- The survey must include an introduction. This should cover the contextual background to the survey, why data is being collected and how it will be used. Respondents should be assured about anonymity, confidentiality (unless a safeguarding concern is identified) and the voluntary nature of their participation.
- You must check to see if your work requires Research Governance approval (for ethical and research methods matters) to proceed. This includes activities to gain additional knowledge routinely obtained from service users, e.g. using surveys, interviews, focus groups, or consultations. This is for the protection of both participants and employees. for more information, please read the research governance process overview.
- If a survey is completed alongside a competition, you must be able to remove the personal details that form the competition entry from the survey. Sometimes a prize is offered as an incentive to complete a survey. In this case, the personal details collected to issue the prize should only be kept for a very short period after the competition has ended. However, the survey itself is likely to be required for a longer period, ensure the two parts can be separated, you can then keep the survey longer without breaching legislation.
- Once your survey responses have been processed into a report, the accuracy of the report is approved, and it is anonymised. There is no reason to hold onto to the original survey returns and the originals can be destroyed at this point.
- You must comply with any retention period you have stated on your privacy notice and ensure you delete any personal information from the survey tool at the stated time. You must not keep information longer than is necessary. This includes information held on third party survey tools. If using an authorised third-party site, follow any guidance on their site to remove data.

8. Information Access and Disclosures

a. Subject Access Requests (SAR)

Under Data Protection Legislation all living individuals have the specified rights, one of which is the right to access their information, generally known as a Subject Access Request.

These requests are dealt with by the Transparency Team within IG, who ensure they are dealt with in line with the statutory requirement of one calendar month. To ensure that the Council can comply with these requests effectively:

- You must not withhold information because you believe it will be misunderstood; instead
- Provide a supporting explanation with the information.
- Provide the information in an “intelligible form”, which includes explaining any codes, acronyms and complex terms.
- The information must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort.
- Arrangement may be made with the requester to view the information on screen or inspect files on our premises.
- You must redact any exempt information from the released documents and explain why that information is being withheld.
- You must not delete or alter personal data in response to a SAR. The Data Protection Legislation defines such alteration as a criminal offence. If you are unsure if personal information should or should not be removed, contact the Transparency Team for advice before taking any action.

b. Requests to amend or delete or stop using personal data held by ECC

The UK GDPR gives an individual a number of rights. They can ask ECC to stop using their personal information, to correct an error and to stop us using it.

If you receive a request to amend or delete an individual’s personal data, you must promptly forward it to DPO@essex.gov.uk to ensure it is dealt with in line with the statutory requirement of one calendar month.

Where this is a request to rectify/amend personal information, taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal information completed, including by means of providing a supplementary statement.

If the data in question records an opinion they are, by their very nature, subjective and it can be difficult to conclude that the record of an opinion is inaccurate. ECC where appropriate may decide that a record is accurate and not to rectify/amend the data.

A request to delete or stop using information must explain why the information being held and used by ECC is wrong or why it is causing them ‘unwarranted and

substantial' distress and they must prove that they are the individual whose data is held and used by us.

These requests are handled in the same manner as a Subject Access Request, however in some cases IG may not agree to the request and will provide an explanation. Here is a list of examples when ECC may not amend/rectify your information:

a. If the processing is necessary;
b. if it is in relation to a contract that the individual has entered;
c. if the individual has asked for something to be done so they can enter into a contract;
d. if the processing is necessary because of a legal obligation (other than a contractual obligation); or
e. if the processing is necessary to protect the individual's "vital interests".

For further information about an individuals rights under the UK GDPR, please see our detailed guidance

c. Freedom of Information (FOI) & Environmental Information Regulations (EIR)

The Freedom of Information Act 2000 and the Environmental Information Regulations 2005 gives members of the public access to any recorded information held by public authorities. They promote transparency.

The Act and Regulations presumes that information should be disclosed unless there is a good reason not to.

As a public authority we are required under the Act to:

- Reply to any request within 20 working days, either by providing the information or stating why it cannot be provided and applying any of the 23 exemptions outlined in the Act.
- Provide advice and assistance to applicants making requests.

For full details on the FOI and EIR guidance use the link.

d. Data Transparency Code

Local Government have a document that sets out the minimum data that local authorities should be publish, the frequency and how it should be published. The Data Transparency Code can be located on the internet.

It is the responsibility of the business to understand what information they handle that falls within the scope of the code and to handle the information accordingly.