|  |  |
| --- | --- |
|  |  |
|  | Information Governance Support  Nottinghamshire County Council in partnership with Essex County Council l |



|  |
| --- |
| **information governance framework** |
| A process for overseeing the performance of the Organisation against a range of Information Governance metrics, analysing the data and feeding it into strategy, policy and risk reviews for continuous improvement |

|  |  |
| --- | --- |
| **Approved by** |  |
| **Date Approved** |  |
| **Version** |  |
| **Review Date** |  |

**Contents**

[A. Copyright Statement 2](#_Toc508358939)

[B. How to use this Framework 3](#_Toc508358940)

[1. Basic Evidence Pack: 3](#_Toc508358941)

[2. Processes: 4](#_Toc508358942)

[3. Report & Review: 4](#_Toc508358943)

[C. Records of Processing Activity 5](#_Toc508358944)

[D. Framework Documentation 6](#_Toc508358945)

[A. Roles & Responsibilities 6](#_Toc508358946)

[B. Reporting & Reviewing 7](#_Toc508358947)

[C. Strategy & Policy 8](#_Toc508358948)

[D. Procedures 9](#_Toc508358949)

[E. Sharing Data with Suppliers and Partners 10](#_Toc508358950)

[F. Statutory Request Templates 11](#_Toc508358951)

[G. Risk Management 12](#_Toc508358952)

[H. Records of Processing Activity 13](#_Toc508358953)

[E. Document Control 14](#_Toc508358954)

# Copyright Statement

All rights reserved, Essex County Council grants its customers who have purchased a licence to use this document for the purposes of the administration and operation of the school to whom it has been sold. For those purposes customers are permitted to use, adapt, publish and copy this document provided that every adapted or published version of this document must include this copyright notice in full. No other use by other organisations or outside the terms of the permitted use stated above is permitted without the prior written permission of Essex County Council. Those infringing Essex County Council’s copyright may be subject to prosecution, claims for damages or other legal action.

Reference made here to ‘the document’ refers to the main Information Governance Framework document and all documents embedded within it, unless the description of the document in Section D makes clear that a document within this framework is the property of another Organisation.

The reference number supplied to you on your License Certificate accompanying this document is your license number which evidences your purchase and confirms your entitlement to use this framework in accordance with the conditions detailed above. This should be quoted to Essex County Council in any challenge to validate the proper use of this documentation.

# How to use this Framework

This framework is designed to be used to demonstrate compliance with Data Protection (and related) law. By using the document templates provided, amending and updating as appropriate, and saving current versions into this main document, this meets and exceeds the requirements under the General Data Protection Regulation (2016) to demonstrate compliance with the Data Protection principles (see [GDPR Art.30](https://gdpr-info.eu/art-30-gdpr/) for details)

Please follow the step-by step guide below to ensure compliance tasks are completed in a logical order. References are links to documents in Section D.

## Basic Evidence Pack:

The following are activities to be undertaken to comply with the requirement to evidence legally compliant processing of personal data

|  |  |
| --- | --- |
| A | Use the documents in Section **A** to determine which individuals will act in the various roles which have responsibility for managing this framework, and which committees or teams will have what responsibilities. |
| B | Use document [**H1**](#_Information_Asset_&) (IAR Tab) to create a list of the categories of record you hold which contain personal data. Use the DLM tab to then record the ways in which you receive and share the information you have identified on the IAR tab, setting clear rules for how the data should be received and sent securely. |
| C | Use document [**H2**](#_Description_of_Organisational) to explain how your technology and how your staff are going to keep personal data secure. Identify the various roles within your organisation and decide what training messages you need to deliver to each and how this will be best delivered. |
| D | Review, adopt and publish the Privacy Notice templates in the appendices of document [**D2**](#_Privacy_Notice) |
| E | Review, adopt and publish the Policies in section [**C**](#_Strategy_&_Policy) |
| F | Review the documentation you have which controls the services delivered to you by your suppliers who handle personal data on your behalf (Contracts, Agreements, Terms & Conditions etc) to ensure you hold appropriate commitments. Ask them for assurance that they comply with Data Protection law (Document [**E7**](#_Letter_to_Data)). |
| G | Ensure you have a current and compliant registration in place with the ICO (Use the templates in document [**D9**](#_ICO_Notification_-)) |
| H | Review the proposed retention rules in document [**D8**](#_Retention_Schedule). Match them to the information assets you have identified in document [**H1**](#_Information_Asset_&) and include the agreed retention periods in your Privacy Notices. |

## Processes:

Processes to successfully manage certain activities where the law requires they are undertaken in a certain way

|  |  |
| --- | --- |
| 1. **Activity Management** | |
| A | Ensure new (or changes to existing) processes which involve personal data are assessed for whether a statutory Data Protection Impact Assessment needs to be undertaken, using documents [**G4**](#_Privacy_Impact_Assessment) & [**G5**](#_Privacy_Impact_Assessment_1) |
| B | Ensure events which meet the criteria of a personal data security incident are handled according to procedure [**D6**](#_Security_Incident_Management) |
| C | When you are considering engaging the services of a supplier to process personal data on your behalf, review the risk of the activity ([**G3**](#_Risk_Treatment_Process)) and determine which of controls in documents [**E1-4**](#_Sharing_Data_with) is appropriate. |
| D | When you are sharing data with another Data Controller, ensure you have captured whether this is lawful and how it should be undertaken in your Data Flows register ([**H1**](#_Information_Asset_&)) and there is an adequate Sharing Protocol in place. |
| E | When you are providing access to personal data to an individual who is not employed by a company with whom you have a contractual relationship, consider use of document [**E6**](#_Non-Disclosure_Agreement) |
| F | When a requestor makes a statutory request for information or to exercise their other rights under Data Protection law, ensure you have considered this appropriately and responded using standard text in documents [**F1-3**](#_Statutory_Request_Templates) |

## Report & Review:

Activities to review the effectiveness of the measures you have in place to comply with the law.

|  |  |
| --- | --- |
| **3. Review** | |
| A | Collect and report data on how well you are managing your personal data activities. Use document [**B1**](#_Reporting_Template) for this. |
| B | Undertake an annual review of your policies which relate to information governance ([**B2**](#_Performance_Reporting_and)) noting changes and approvals in document [**D1**](#_Policy_Change_Log) |
| C | Undertake an annual review of your personal data risks ([**B2**](#_Reporting_&_Reviewing)) using [**G2**](#_Risk_Assessment) to initially assess risks, [**G3**](#_Risk_Treatment_Process) to rate risks, and [**G1**](#_Corporate_Risk_Register) to gather, manage and present risks |
| D | Undertake an annual review of your contracts with suppliers to ensure they are being complied with |
| E | Undertake an annual review of the effectiveness of information governance training, using staff feedback and analysing the nature and frequency of security incidents ([**B1**](#_Reporting_Template)). |
| F | Undertake a review of you CCTV processes (if applicable) using the procedures in document ([**D5**](#_Surveillance_Management)) |
| G | Ensure the content of your registration with the ICO has been reviewed as part of the process for making the required ICO annual payment ([**D9**](#_ICO_Notification_-)) |
| H | Ensure your Data Protection Officer has reviewed and commented on the review outcomes before they are reported to a governing body. |

# Records of Processing Activity

|  |  |  |
| --- | --- | --- |
| Data Controller | [Organisation Name] | |
| Contact Details | Address |  |
| Phone |  |
| Email |  |
| Website |  |
| Data Protection Officer | [Employee Name/ Outsourced Supplier Employee Name] | |
| Purposes of processing | The purposes for which personal data is processed are detailed within the Organisation’s Privacy Notices provided below ([**Section** **D, D2**](#_Privacy_Notice)) | |
| Description of the categories of: | | |
| Individuals | This information is detailed in the Organisation’s entry on the Register of Data Controllers available at this weblink [Insert hyperlink to Register entry]. This is supplemented by detail in the Information Asset and Data Lifecycle Mapping Register provided below ([**Section D, H1**](#_Information_Asset_&)) | |
| Personal Data |
| Recipients |
| Details of transfers to third countries | This information is detailed in the Information Asset and Data Lifecycle Mapping Register provided below ([**Section D, H1**](#_Information_Asset_&)) and is included in the Organisation’s Privacy Notices ([**Section D, D2**](#_Privacy_Notice)) | |
| Retention schedule | Our retention schedule is provided below ([**Section D, D7**](#_Retention_Schedule)) with key retention practices published on our Privacy Notices ([**Section D, D2**](#_Privacy_Notice)) | |
| Description of Technical and Organisational Security Measures | An outline of our technical and organisational security measures is provided below ([**Section D, H2**](#_Description_of_Organisational)) | |

# Framework Documentation

In this section you will find embedded document templates which support tasks explained above in the step-by-step compliance guide (Section B)

All documents should be reviewed, amended if necessary and all current versions should be saved back into this document under the appropriate reference. This then ensures that this Framework is a current, complete and accurate description of how you process Personal Data in your School, and can be presented to the regulator if requested as evidence of your legal compliance.

|  |  |  |
| --- | --- | --- |
| Roles & Responsibilities | | |
| 1 |  | Senior Information Risk Owner (SIRO): Role Profile |
|  |  | Defined responsibilities of the SIRO to be used in addition to an existing substantive role profile. Usually this is a Headteacher’s role. |
| 2 |  | Data Protection Officer (DPO): Role Profile |
|  |  | Defined responsibilities of the DPO to be used in addition to an existing substantive role profile or to held understand and work with an outsourced or shared role. |
| 3 |  | Information Champion: Role Profile |
|  |  | Defined responsibilities of Information Champions to be used in addition to an existing substantive role profile, if the organisation decides that it wants a network of staff with additional responsibilities in this area. |
| 4 |  | Information Governance Board: Terms of Reference |
|  |  | Defined role of the Information Governance Board. Can be wholly the responsibility of a group such as Senior Leadership Team, Full Governors, or a Governors Sub-Committee, the responsibilities can be shared between the various groups. |
| 5 |  | Data Protection Officer (DPO) Activities |
|  |  | A summary of the main activities to be provided by a Data Protection Officer. |
| 6 |  | |  | | --- | | NCC Data Protection Officer (DPO) – Responsibility Profile | | This DPO responsibility profile produced by Nottinghamshire County Council sets out the minimum duties to be incorporated into an existing school role. | |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Reporting & Reviewing | | |
| 1 |  | Reporting Template |
|  |  | A comprehensive overview of Information Governance performance data for review, analysis and action planning |
| 2 |  | Performance Reporting and Reviewing |
|  |  | Detailing the processes in place to monitor information governance performance and to review the effectiveness of the governance framework |
| 3 | Embed Here | Report Examples |
|  |  | Examples of Reports and minuted evidence of meetings at which the reports were reviewed. Please embed copies of these documents as evidence of your information governance framework in action. |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Strategy & Policy | | |
| 1 |  | Information Governance Strategy |
|  |  | A strategy document providing a methodology for implementing solutions to improve and maintain Information Law compliance |
| 2 |  | Information Governance Framework Policy |
|  |  | Supporting effective corporate management of Information Governance activities; including key roles and strategic policy and risk reviews |
| 3 |  | Data Protection |
|  |  | General rules in complying with Data Protection law |
| 4 |  | Statutory Requests |
|  |  | Requirements for managing requests for information to comply with the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations (EIR), the Data Protection Act 1998 (DPA) and from 25th May 2018 the General Data Protection Regulations 2016 |
| 5 |  | Acceptable Personal Use |
|  |  | Explaining what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use |
| 6 |  | Data Handling Security |
|  |  | Responsibilities for managing IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations |
| 7 |  | Security Incidents |
|  |  | Responsibilities for reporting and investigating breaches of Information Governance policy, including reporting to the Regulator |
| 8 |  | Records Management |
|  |  | Responsibilities for management of information to support secure access and effective retention, destruction and preservation processes |
| 9 |  | Policy Template |
|  |  | Template document for consistent management of additional policies |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Procedures | | |
| 1 |  | Policy Change Log |
|  |  | For managing changes to policies over time, approval recording and publication to the Organisation |
| 2 |  | Privacy Notice |
|  |  | Ensuring Data Subjects are well-informed about the why their personal data is necessary and how it will be managed in line with their statutory rights |
| 3 |  | Consent |
|  |  | Ensuring processing under consent is appropriate and that the quality of consent is compliant with the law |
| 4 |  | Personal Data Minimisation |
|  |  | Ensuring the processing of personal data is kept to a necessary minimum in accordance with the law |
| 5 |  | Surveillance Management |
|  |  | Ensuring effective processes are in place for the management of equipment which records personal data in video in accordance with the law and relevant codes of practice |
| 6 |  | Security Incident Management |
|  |  | The process of investigating and managing instances of breaches of Information Governance policy |
| 7 |  | Records Management Best Practice Guide |
|  |  | Guidance published by the Information & Records Management Society (IRMS) on best practice for managing records, including a list of the main record types held by schools and their associated retention management provisions. *This document is owned by* [*IRMS*](http://irms.org.uk/). |
| 8 |  | Retention Schedule |
|  |  | Template for publishing an approved set of retention rules. Content is derived from the IRMS document above. |
| 9 |  | ICO Notification - Register of Data Controllers |
|  |  | Standard details provided by the ICO for Data Controllers to describe the nature of their personal data processing. *This document content is owned by the* [*ICO*](https://ico.org.uk/for-organisations/register/nature-of-work/). |
| 10 |  | Procedures Template |
|  |  | Template document for consistent management of additional procedures |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Sharing Data with Suppliers and Partners | | |
| 1 |  | Contract Schedule |
|  |  | Standard clauses to provide basic contractual controls over Data Processor compliance with information law |
| 2 |  | Third Party Information Policy Requirements |
|  |  | Complementing the contractual clauses with additional agreement from Data Processors to comply with key Organisation policies |
| 3 |  | Procurement Stage 1 |
|  |  | This document should be completed by all bidders for procurement exercises relating to services which process personal data. |
| 4 |  | Procurement Stage 2 |
|  |  | This document should be completed by all preferred bidders involved in procurement activities which have been categorised as high risk data processing |
| 5 |  | Information Sharing Protocol |
|  |  | A template for public agreements for personal data sharing with partners through the Whole Essex Information Sharing Framework. For use where there is no existing sharing agreement and one therefore needs to be initiated. *This document is owned by* [*WEISF*](https://weisf.essex.gov.uk/)*.* |
| 6 |  | Non-Disclosure Agreement |
|  |  | Confidentiality agreement for individuals not employed by an organisation with whom a contract or similar agreement exists |
| 7 |  | Letter to Data Processors |
|  |  | Standard text to communicate to Data Processors your need for their assurance over compliance with Data Protection law |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Statutory Request Templates | | |
| 1 |  | Freedom of Information Requests |
|  |  | Response Templates for Requests made under the Freedom of Information Act (2000). Use these standard responses as a basis for ensuring compliance with the law. |
| 2 |  | Environmental Information Regulations Requests |
|  |  | Response Templates for Requests made under the Environmental Information Regulations (2004). Use these standard responses as a basis for ensuring compliance with the law. |
| 3 |  | Subject Access Requests |
|  |  | Response Templates for Requests made under the Data Protection Act (1998) and the General Data Protection Regulations (2016). Use these standard responses as a basis for ensuring compliance with the law. |
| 4 |  | Model Publication Scheme |
|  |  | A standard form to describe what information you will routinely publish or make available on request. *This document is owned by* [*ICO.*](https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/) |
| 5 |  | Publication Scheme Data |
|  |  | Suggested content for information you may choose to make available through your Publication Scheme. |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Risk Management | | |
| 1 |  | Corporate Risk Register |
|  |  | A register which provides an overview of all corporate risks, their ratings, how they are to be managed and who is responsible for doing so. This document supports an annual risk review activity |
| 2 |  | Risk Assessment |
|  |  | Where a new risk has been identified, it can be articulated via this form and presented to the appropriate board or role for an assessment on how best to manage it. This is a mechanism for adding a new risk to the Corporate Risk Register |
| 3 |  | Risk Treatment Process |
|  |  | A consistent scheme for formally rating Information Governance risks |
| 4 |  | Privacy Impact Assessment Template |
|  |  | Use this form to capture the privacy issues of new (or changes to existing) activities which involve the processing of personal data, and to record approvals or rejections. The form can also be used to manage Data Protection Impact Assessments for ‘high risk’ processing under the GDPR |
| 5 |  | Privacy Impact Assessment Guidance |
|  |  | Reference and guidance document to support completion of Privacy Impact Assessment forms |
| 6 |  | Privacy Impact Assessment Example |
|  |  | An example completed assessment covering Capita SIMs |

[Back to Section B](#_How_to_use)

|  |  |  |
| --- | --- | --- |
| Records of Processing Activity | | |
| 1 |  | Information Asset & Data Flow Mapping Register |
|  |  | Use to capture and review data for an Information Asset Register and Data Flow Mapping. Assign owners and record other metadata about the information you hold and process as assurance evidence to a regulator, as a risk management tool and a useful business efficiency aid |
| 2 |  | Description of Organisational & Technical Security Measures |
|  |  | Outline of the measures adopted to comply with Principle 6 of the General Data Protection Regulations |

[Back to Section B](#_How_to_use)

# Document Control

Changes in this version

|  |  |  |
| --- | --- | --- |
| **Section** | **Change Type** | **Details** |
| B | New | Created internal document hyperlinks from Section B content to documents in Section D |
| All | New | Formatted with joint NCC/ECC branding |