Connect,
Learn & Grow

Frinton-on-Sea Primary School

GDPR

RECORDS MANAGEMENT POLICY

Approved by	Full Governing Body
Date Approved	Summer 2021
Version	1.1
Review Date	Summer 2022

Responsibilities for management of information to support secure access and effective retention, destruction and preservation processes

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: You must **document** your work activities in line with procedures
2. ***MUST***: You must store all work information in the format and **medium** best suited to its use in line with procedures
3. ***MUST***: You must ensure that the information you manage is only known to an **appropriate audience**
4. ***MUST***: All information in any format which we hold as a record of our activity must be **retained** after 'closure' in line with Retention Guidelines
5. ***MUST***: Owners must regularly **review** information in line with Retention Guidelines to make best use of the available storage space
6. ***MUST***: We must **monitor** the success of the review process to maintain compliance with the law
7. ***MUST***: You must manage Pupil records in line with best practice and specific system **guidance**
8. ***MUST***: You must follow Good Practice for Managing E-Mail when storing **emails** as records
9. ***MUST***: We must ensure that the **facilities** available for storing and managing information meet legal requirements and best practice
10. ***MUST***: We must maintain a **selection procedure** for identifying, reviewing and managing records with **historical value**
11. ***MUST NOT***: You must not store business information on a **personal drive** or on equipment not provided by the Organisation
12. ***MUST***: All Information **Assets** identified on the Register must be associated with a retention period from the Retention Guidelines.
13. ***MUST***: The Retention Guidelines must be reviewed for **changes** in legislation and the Organisation's business needs.
14. ***MUST:*** When archiving paper records, information on ownership, retention and indexing quality must be recorded.
15. ***MUST NOT:*** You must not use the archive storage services of any other commercial company than the **approved supplier**

Why must I do it?

- These measures ensure Organisation information, where appropriate to do so, is shared effectively to support efficient business processes and maintain effective service delivery to customers.
- Managing records in line with the best practice guidance fulfils duties under the section 46 Code of Practice on Records Management under the Freedom of Information Act 2000. Retention Guidelines are published so there is clear communication to customers over what information should still be available to them if they wish to make a request. To retain information too long or to destroy too soon leaves us open to criticisms on openness and transparency, and in some cases, compliance with the law.
- In order to comply with the Section 46 Code of Practice (see above) we must ensure that we are destroying all related information across all formats. For example, destroying a paper file on a project but keeping all the electronic documents about the project in a shared network folder can cause problems if a Freedom of Information request is received. The request co-ordinator assumes that as the paper file is destroyed then we do not hold any information and responds accordingly. We would then be in breach of the act.

How must I do it?

1. Employees are aware of best practice requirements and any guidance on use of specific systems through training and communications
2. Employees are aware of best practice requirements and any guidance on use of specific systems through training and communications
3. You must ensure that paper files are accessible to authorised colleagues in your absence, by ensuring others know where to find keys to lockable storage areas. You must be aware of who information should be shared with, and ensure it is only shared with that audience. You must ensure that you save electronic information in a shared environment, but with appropriate access controls if the information has a restricted audience.
4. Follow the best practice guidance and any superseding amendments made by the Organisation
5. Follow the best practice guidance and any superseding amendments made by the Organisation
6. Designated employees must gather performance data on activities within the scope of this policy for review by the Data Protection Officer and the Leadership Team
7. Follow the best practice guidance and any superseding amendments made by the Organisation
8. Follow the best practice guidance and any superseding amendments made by the Organisation
9. The organisation must approve and regular review facilities such as systems and physical storage as appropriate against security requirements in Data Protection Law, and all employees must help maintain security standards by following procedure.
10. Records can be identified for preservation at any point in the records lifecycle, but will not transfer until we have no ongoing administrative need (i.e. at the end of a retention period). When information is due to be destroyed, there should be a final review to select records for transfer to the Essex Record Office.
11. By only storing all business information on the relevant systems designated by the Organisation and by using only equipment approved by the Organisation.
12. The Information Asset Owner is responsible for ensuring that Information Asset Managers amend entries on the Information Asset Register to show the correct retention period from the schedule.
13. A policy review (at least annually) must review the provisions of best practice retention guidance and make any necessary amendments, documenting the reasons for change and managing affected records accordingly.
14. We must complete and retain archiving indexes providing the relevant information about paper records in storage, ensuring that the Organisation is aware of what information it holds at all times and when they can be reviewed.
15. Any use of a commercial storage provider must be assessed and approved to ensure the right security and financial provisions are place. Use of alternatives that have not been approved may not provide value for money and may not provide secure services.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Mrs T. Caffull, Executive Head Teacher

References

- Data Protection Act 2018
- Article 8, The Human Rights Act 1998
- Freedom of Information Act 2000 (FOIA).
- Code of Practice on Records Management (under Section 46 of the FoIA)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.