



Records Management Policy

Policy Number - 41

Document Management Information

Applicable to:	All staff, students, Trustees, Members of the Trust and members of the public who may request information
Dissemination:	Trust website, NET Frameworks and Policies for all staff Teams
Linked policies:	Data Protection Policy Freedom of Information (FOI) Policy Acceptable Use Policy Appropriate Data Policy Child Protection & Safeguarding Policy
Implementation:	Trust wide through Trust Leaders
Training:	GDPR UK - Education (iHasco) – All Staff
Review Frequency:	3 years
Policy Author:	Data Protection Officer (DPO)
Policy Lead:	Director of Operations
Approval by:	Audit and Risk Committee
Approval Date:	29 November 2023
Next Review Due:	Autumn 2023

Revision History

Document version:	Description of Revision:	Date Approved:
1	New Policy	29 November 2023

CONTENTS

1. AIMS AND INTRODUCTION	3
2. SCOPE OF THE POLICY	3
3. RESPONSIBILITY	3
4. TRANSFERRING OF PUPIL RECORDS	4
5. MANAGING CONFIDENTIAL WASTE	4
6. METHODS OF DISPOSAL	4
7. INDIVIDUAL RESPONSIBILITY	5

1. AIMS AND INTRODUCTION

Nene Education Trust (the "Trust" including its schools/academies; 5Wells; Manor Sports and Leisure) recognises that efficiently managing its records is essential to be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the organisation. Records provide evidence for meeting legal obligations and protecting interests of the Trust and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

The Trust has adopted the Information Management Toolkit for Schools created by IRMS (Information and Records Management Society) and adheres to its principles and guidance with the retention schedule. A copy of this document is available on request and included within the Policies Framework folder.

Section 46 of the Freedom of Information (FOI) Act 2000 requires schools to follow a Code of Practice on managing their records. Under Section 7 of the Code of Practice on the Management of Records, it states that: "Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy."

Educational records include information about pupils and former pupils:

- Processed by, or on behalf of, the Trust (including its schools) or a teacher.
- Originating from or supplied by Local Authority employees (for certain schools).
- Originating from or supplied by teachers or other employees of the school.

Data will be retained for no longer than necessary for the purpose or purposes for which it was collected. All steps will be reasonably taken to securely destroy or erase from systems, all data and records which are no longer required.

2. SCOPE OF THE POLICY

This policy applies to all records that are created, received or maintained by staff of the Trust and all its schools in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the Trust and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

A small percentage of the Trust or school's records may be selected for permanent preservation as part of the institution's archives and for historical research.

Records processed by a teacher solely for the teacher's own use will be excluded from pupils' educational records.

3. RESPONSIBILITY

Under the UK General Data Protection Regulation (UK GDPR), the Trust and schools are responsible for ensuring that the collation, retention, storage and security of all personal information they produce, and hold, meets the provisions of the UK GDPR. This includes:

- Personal information appearing in a pupil's educational record.
- Any other information they hold which identifies individuals, including pupils, staff and parents/carers.

The Trust is registered as a Data Controller with the Information Commissioner's Office (ICO).

The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Chief Executive Officer (CEO). The Data Protection Officer (DPO) will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely manner. The lawful basis for processing data will be recorded by the Trust.

Individual staff must ensure that records for which they are responsible, are accurate; maintained and disposed of in accordance with the Trust's records management guidelines.

Personal data will not be retained for no longer than required which includes emails which have been actioned. Examples include:

- A parent notifies the school their child is absent, this is recorded on the school Management Information System (MIS), so the email is immediately deleted.
- A gym user books onto a class. The email is retained to confirm the booking and invoice for the class attendance; then deleted as no longer required.
- A staff member receives an email regarding a Special Educational Needs and Disability (SEND) pupil from the Local Authority (LA). The email is saved to Office 365 or school management recording system; then the email is securely deleted as no longer required.
- A booking is received for a course, once logged and invoiced, the email is securely deleted.

4. TRANSFERRING OF PUPIL RECORDS

Principals must ensure the statutory requirements for the transfer of records between schools are fulfilled, including the completion of the Common Transfer File (CTF). This is noted in the Education (Pupil Information) (England) Regulations 2005, SI 2005/1437. Academies are not subject to these regulations, however, they are expected to adhere to the following protocols, as a matter of good practice.

If a pupil moves to another school in England; Wales; Scotland; or Northern Ireland, the pupil's CTF and educational record must be transferred securely to the new school.

The means of transfer to a school outside England must be in line with the arrangements for transfer between schools in England. Information must be transferred within 15 school days of any request from the pupil's new school. The pupil's CTF should be sent to the new school either:

- a) Through the school to school (s2s) secure file transfer system.
- b) Over a secure network that can only be accessed by the LA, the governing body or a teacher at any school within that LA. If the new school is unknown, the Department for Education recommends that the school should still complete the CTF and load it onto s2s. Where a CTF has not been received for a new pupil, a request can be made to the LA to search for the files on s2s.

Some LAs transfer pupil paper files between schools. However, for transfers to other LAs, it is recommended that records are signed for.

Requests to transfer a pupil file outside the UK because a pupil has moved into that area, must be referred to the LA for further advice.

5. MANAGING CONFIDENTIAL WASTE

- This should be made available for collection in the confidential waste bins or sacks located around the school/offices.
- Anything that contains personal information must be treated as confidential.
- Where deleting electronically (including emails and files), please refer to the Trust GDPR Lead, or GDPR Lead in the school, to ensure that this is carried out effectively.
- Further guidance regarding the disposal of confidential waste can be found in the section below.

RECORDS CONTAINING PERSONAL DATA MUST NOT BE PUT WITH REGULAR WASTE OR INTO A SKIP, EVEN WHEN SHREDDED.

6. METHODS OF DISPOSAL

Records containing personal data should be made either unreadable or cannot be reconstructed. This includes paper records and all other media. Electronic data should be archived on electronic media and deleted appropriately at the end of the retention period.

This means:

- Shred paper records using a cross-cutting shredder.
- Use a wastepaper merchant to bundle up and dispose of any other records.
- For IT waste, speak with the IT provider for the Trust who will advise on the most secure method for destruction or deletion.

Where an external contractor is used for shredding records, it is recommended that all records must be shredded on-site in the presence of a staff member. The organisation must also be able to prove that the records have been destroyed by the company, who should provide a certificate of destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

7. INDIVIDUAL RESPONSIBILITY

Much of the retention and deletion of documents will be automatic, but when faced with a decision about an individual document, an individual should ask yourself the following:

- Has the information come to the end of its useful life and why I am holding it? This includes emails if information is saved elsewhere and/or no longer required.
- Is there a legal requirement to keep this information or document for a set period?
- Would the information be likely to be needed in the case of any legal proceedings? In particular, is it potentially relevant to an historic child abuse enquiry?
- Is the information contentious, does it relate to an incident that could potentially give rise to proceedings?
- Would the document be useful for the organisation as a precedent, learning document, or for performance management processes?
- Is the document of historic or statistical significance?