Handling of Safeguarding files

Published: July 2025

OUR VISION

Our vision is to provide pupils with the confidence, skills and ambition to achieve a successful and productive life. We aim to ensure they leave the school with a 'new day, new opportunity' ethos and are capable of becoming positive members of their communities. To do this, we have 3 principles that underpin our policies, practices and everything we do:

- Everyone can learn, achieve and has the potential to be successful
- Positive relationships are key to success and are underpinned by mutual trust, respect and caring for one another
- We have high expectations in everything we do

Policy owner	White Trees School	**Last review**	July 2026
Date Created	July 2025	**Next review**	July 2027

Part of the White Trees group
Building Brighter Futures

Introduction

The aim of this policy is to provide guidance to staff when receiving safeguarding files. The policy aims to support staff in ensuring the appropriate procedures are in place. This includes where to store the files and information on retention.

Only Staff with Level 3 safeguarding are able to access and read through the filles.

1. Receipt of Files via Post

All safeguarding and student information files must be addressed to the Designated Safeguarding Lead (DSL) or Deputy Head and delivered directly to the **School Site office.**

Initial Handling:

Office staff must open post securely and verify that the contents relate to safeguarding files. Staff will be required to Log the receipt in the **Safeguarding File Receipt Log**, including:

- Student's name and date of birth.
- Date received.
- Sender (previous school or agency).
- Type of file received.
- Name of the staff member who opened/handled the post.

2. SENCO/DSL Access

- SENCO or DSL accesses the file in a private, secure area.
- DSL to upload relevant information to CPOMS including the appropriate safeguarding SEND tags

Must log:

- Date/time of access.
- Their name and role.
- Any immediate safeguarding/SEND actions require

Timely processing is crucial. **Upload must be within 3 working days of receipt** SENCO or DSL - The whole file must be uploaded to CPOMS, appropriately labelled, and recorded in both the audit trail and destruction log.(refer to sections 3, 4 and 6 below.

- ❖ **DSL or SENCO holds ongoing responsibility until upload.**

3. Secure Storage (Online)

- Once scanned, safeguarding and student information files must be stored digitally on a **secure, access-controlled platform** using CPOMS. Files must be:
    - Clearly labelled and categorised (e.g., “Safeguarding)
    - Stored in **non-editable formats** (e.g. PDF).
    - Accessible only to authorised safeguarding personnel (SENCO, DSL, Executive Headteacher).
- ❖ Regular backups must be in place, and data protection measures must meet GDPR standards.

Retention:

Digitally stored safeguarding records must be retained **until the student’s 25th birthday, however files relating to child sexual abuse should be retained untill the childs 75th birthday.**
in accordance with Department for Education (DfE) and IRMS guidance.

4. Handling Log & Audit Trail

A **Safeguarding File Handling Log** must be maintained (preferably a shared digital log for auditability), capturing:

Date	Action	Staff Member	Notes
01/05/25	File received via post	Admin Officer Jane Smith	From ABC Primary
02/05/25	Delivered to SENCO	John Doe	For review
03/05/25	Returned to HO	Jane Smith	Via secure courier
04/05/25	Scanned to CPOMS	Admin Officer Amy Lee	Upload complete
Retention	File stored securely	-	To be retained until 2038

If the files are delivered to HO then they must be Securely Transferred Files should be hand-delivered by a trusted staff member from the Business team who holds SafeguardingLevel3certification.

Log:

- Date of internal transfer.
- Staff member delivering and receiving.
- Signature confirmation on both ends.
-

5. Destroying Physical Safeguarding Files (Post-Digitisation)

-Confirm Files Are Safely Stored Digitally

Before destroying any paper files:

- Ensure the safeguarding record is **fully scanned** (all pages, legible, complete)
- Stored on a **secure, encrypted platform** such as **CPOMS** or equivalent
- DSL has checked digital version and confirms it's the full record

Check Retention Guidance

- Must **retain safeguarding records until the child is 25**

  Storing them **digitally** is acceptable — physical files can be destroyed *only if*:

  - The scanned copy is complete and safe
  - Your **school/MAT data protection policy allows this**
  - The **DPO or DSL has authorised it**

Complete a Safeguarding File Destruction Log

Keep a formal log that includes:

- Pupils Name
- UPN
- DOB
- Date Scanned
- Staff of who scanned
- Authorised by

- Date of destruction
- Method (e.g. shredded)

This should be signed off by the DSL and filed securely (paper or digital is fine).

- **Destroy Files Securely**
- Use a cross-cut shredder
- OR use a GDPR-compliance, licensed confidential waste service

❖ **Destruction must be logged and auditable for Ofsted, local authority audits, or legal requests.**

Published on	
By	
Chair of Gov Sig/Date	
Head Teacher Sig/Date	

WhiteTrees independent school

WhiteTrees group
Building Brighter Futures