

## Nottinghamshire Child Protection and Confidential File Self-Audit Supporting Guidance 2025-2026

This guidance explains **why** completing the annual self-audit is essential and sets out the **minimum evidence standards** for child protection record-keeping, lawful information sharing, and **secure, timely transfer** of child protection files. It complements (not repeats) **KCSIE 2025** and local NSCP procedures. (*KCSIE Summary; Part Two 76–79*)

### Why this audit matters

Safeguarding is a statutory duty and an organisational accountability. Governing bodies and proprietors must be able to **assure, with evidence**, that their school or college keeps children safe through robust policies and **reliable, timely records** of concerns, decisions, and actions. (*Part Two 76–79*)

Child-centred practice depends on **early action, lawful information sharing**, and **clear files** that show what happened, why, and with what outcome. Where records are incomplete, late, or unclear, risks escalate and opportunities to protect children are missed; recurring learning in practice reviews highlights **poor record-keeping and slow information sharing** as common failings. (*Part One 49–55, 66–68*)

Completing the audit is therefore not a paperwork exercise: it is a **risk-reduction tool** that surfaces gaps, prompts corrective actions, and provides governance with defensible assurance that the setting meets KCSIE 2025 expectations. (*Part Two 94–101*)

### What good child protection record-keeping looks like

Every child who is the subject of safeguarding concerns must have a separate, confidential child protection file (paper or electronic) that is stored securely and accessed strictly on a need-to-know basis. The file should contain a factual summary of the concern (using the child's words where possible), the dates, times and people involved, the actions taken, the decisions and rationale, and the outcomes, maintained in a clear chronology. (*Part One 66–67; Annex C 173–177*)

Information-sharing entries should record what was shared, with whom, when, and under which lawful basis, noting any special category data considerations and why sharing without consent was justified if consent was not appropriate or would have increased risk. (*Part Two 114–120, esp. 118–120*)

The DSL (and deputies) should implement regular quality assurance, for example, termly spot-checks on files, to correct gaps, standardise entries, and ensure files are ready for transfer at short notice. Evidence of this QA (date, sample, findings, actions) should be retained for audit and governance challenge. (*Annex C 173–177; Part Two 94–101*)

### Lawful information sharing in practice

Schools and colleges **can and should** share information to keep children safe; **DPA 2018 and UK GDPR do not prevent this**. Staff should be proactive and **share early and proportionately** when risks emerge, recording the decision and its legal basis. Where consent cannot reasonably be obtained, or obtaining it would **place a child at risk**, sharing **without consent** is lawful and appropriate. (*Part Two 114–120, esp. 119–120*)

In all cases, the record must show **what was shared, with whom, when, and why**, and how the decision aligned to **local multi-agency thresholds**. If in doubt, staff should consult the DSL promptly rather than delay action. (*Part Two 114–118, 106–113*)

## Transferring child protection files and supporting transition

When a child moves setting, the **child protection file must be transferred within five school days** for in-year moves, or within the **first five days of a new term**. The file must travel **separately from the main pupil file**, using **secure transit** (encrypted digital or sealed courier), and the sending DSL must obtain **confirmation of receipt** from the receiving DSL. *(Part Two 121–122)*

Where appropriate, the DSL should **share essential advance information**, so support is **in place on arrival** (for example, for a survivor of abuse or a child supported through Channel), and ensure **key staff** at the destination (DSL, SENCO/named SEND) are aware. High-risk transitions (Year 11→12, managed moves, exclusions, moves into/out of Alternative Provision, and returns from prolonged absence) require particular care, with records showing early planning, clear risks, and agreed actions. *(Part Two 121–122, 168–171, 177)*

## Recording child-on-child sexual violence and sexual harassment

For any report or sign of child-on-child sexual violence or sexual harassment, the initial record should capture **facts only** in the child's words, avoid opinion, and note who was present. **Do not promise confidentiality**. The DSL must complete an **immediate risk and needs assessment**, and where rape or assault by penetration is reported, the setting should **remove the alleged perpetrator from shared classes** and manage proximity on site and transport while decisions progress. *(Part Five 471–474, 484–488, 125)*

The record should show the **chosen response route** (managed internally, early help, referral to children's social care, and/or police) and the **support pathways** for the victim (for example, ChISVA/SARC and mental health support), with regular **review updates**. *(Part Five 489–519, 535–536)*

## Online safety oversight records

The DSL **leads safeguarding including online safety** and must **understand and oversee filtering and monitoring** arrangements, including how concerns are flagged and escalated. Settings should complete an **annual effectiveness review** against the DfE filtering and monitoring standards, avoid unreasonable over-blocking, and retain a concise **incident and actions log** to evidence oversight. The child protection policy should explicitly cover **mobile/smart technology** on site (3G/4G/5G). *(Part Two 102–105, 134–143, 137, 140–143)*

## High-risk placements, attendance and EHE: minimum evidence

Where a child is educated in **Alternative Provision**, the placing school remains responsible for safeguarding and should hold **written confirmation of staff checks**, records of **site addresses** (including subcontracted or satellite sites), and evidence of **reviews at least half-termly**, acting immediately on concerns. *(Part Two 168–171; Part Three 331)*

**Persistent absence** and **children missing education** must be treated as safeguarding warnings, with records showing **>1 emergency contact**, early help/escalation and **joint plans** with children's social care where indicated. For **Elective Home Education**, settings should minute a **pre-withdrawal multi-agency meeting** for vulnerable children and **notify the local authority** when removing from roll. *(Part Two 101, 177–181)*

## Governance and equality

Senior leaders and governors should maintain a **termly oversight log** noting completion of the audit, **file transfer timeliness**, information-sharing decisions, **online-safety review outcomes**, AP reviews, attendance/CME escalations, and EHE meetings. Logs should also show how **Equality and Public Sector Equality Duty** considerations are applied (particularly monitoring and responding to **sexual and racist harassment**) as part of safeguarding assurance. *(Part Two 84–91, 94–101)*

## How to complete the audit

Details on how to prepare for and complete the audit can be found within the first section of the audit tool.

For further advice and information, or should you have any queries please contact the Safeguarding Children in Education Officer – Zain Iqbal / [zain.iqbal@nottsccl.gov.uk](mailto:zain.iqbal@nottsccl.gov.uk)