Safeguarding Storage and Communication

Aim

After the study of the safeguarding audit this DPIA will review the different types of personal data found within hard and electronic copies of safeguarding files along with assessing the risks of how information is communicated and accessed by authorised persons and suggest ways to reduce all processes to low or minimal risk.

Data Processing

About the handling of the data - How will you collect, use, share, store and delete data?

Data will be collected from internal and external sources including the previous setting, and multi-agency work.

About the data – quantity of data, timeframe, and type. reference special category data.

Safeguarding files explicit to each child/family. This could include Multi Agency referral forms (MARF), Children in Need (CIN), Team around the Child (TAC) or Case conference minutes. Observations may also be recorded by staff and external agencies. Specialist data such as medical history will also be recorded.

The safeguarding files will be kept until the age of 25/until the child moves to secondary school and a one page chronology will kept until the age of 25. The chronology will be kept in case a file is lost or in case a complaint is made regarding the schools work to support the child/family.

About the data subjects – Expectations and control? Reference vulnerable groups and existing concerns over current processing?

Only authorised personnel; Designated Safeguarding Lead (DSL) and Deputy Safeguarding Leads (DDSL) will have access to the child's/family's safeguarding files. The communication of this information will be conducted through secure mechanisms e.g. EGRESS to multi agencies who have direct impact with the child/family.

Identify benefits of the processing?

Ensure all vulnerable pupils are cared for appropriately and action can be taken quickly and effectively.

Consultation

No consultation is required as this falls within the remit of Keeping Children Safe in Education (KCSIE) September 2024 (statutory by law).

Compliance Consideration

The majority of our processing will be done under the public task and vital interest umbrella.

The safeguarding policy will be clearly communicated, documented and shared with all, therefore, functional creep should not be an issue.

Assess Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Safeguarding information	High	High	High
Medical Information	High	High	High
Personal information (name, address, DOB)	Medium	Medium	Medium
External Agency names and work addresses	Low	Low	Low

Measures to Reduce Risks

Risk	Options to reduce or eliminate risk	Risk Eliminated/ Reduced/ Accepted	Residual Risk	Measure Approved
Loss of Safeguarding File	Access only granted to DSL and DDSL's and upon withdrawal of a file from the cabinet this must be logged on the sheet which is held inside the door of the cabinet. Upon return this will also be logged.	Accepted	Medium	Yes
Safeguarding information sent via email to an incorrect recipient	All safeguarding information that is communicated to an external agency must be facilitated through a secure mechanism e.g. EGRESS.	Accepted	High	Yes
Internal safeguarding referral not presented to the DSL/DDSL in the appropriate manner	Safeguarding policy communicated effectively and procedures are firmly in place for staff to follow. Safeguarding training to be conducted annually with staff.	Accepted	High	Yes
Photocopied safeguarding documents left on the photocopier/printer	All photocopying/printing should be under 'secure print' processes. Therefore, staff cannot print or photocopy documents without being at the photocopier.	Eliminated	High	Yes

Safeguarding documents not filed appropriately e.g. left on a desk overnight	Clear desk policy and procedures are made clear through the safeguarding policy and training. DSL office locked whenever they are not present within the room.	Accepted	High	Yes
Safeguarding files accessed by unauthorised personnel.	Only the DSL and DDSL have access to the locked filing cabinet. The key and security processes are only known by those with authorisation.	Eliminated	High	Yes
Secure transfer of file to the next setting	Under KCSIE Sept 2024 files should be transferred either in person, collected or electronically e.g. CPOMs. In all cases a receipt is required from the receiving school.	Eliminated	High	Yes

Policy Reviewed **May 2024**
Next Review Due **May 2026**