|  |  |
| --- | --- |
| Caldecott Fostering Online Safety Policy: Information Protection and Access | Document OLS-06Reviewed 09.02.2024 |
| Authorised by:Jackie Neil (registered manager) |  |

**Policy Statements**

1. Access to the Internet and other communications MUST be controlled. This MUST be appropriate for the age or specific circumstances of the child.
2. Technical controls SHALL be applied where technically feasible.
3. Staff, volunteers and carers MUST manage and protect personal information in accordance with current data protection legislation.
4. Staff, volunteers and carers MUST process personal information in accordance with the professional methods currently prescribed by the Registered Manager.
5. Data breaches MUST be reported via Caldecott’s Incident Reporting process.
6. On the cessation of a placement all personal data, whether digital or physical, that pertains to the care of the child or young person MUST be returned to the agency by the carer with copies permanently deleted.

**Process/Control Description**

Access to the Internet and other technological communications should be managed as appropriate to the age and maturity of the child. Restricting access to devices may be appropriate in some circumstances where time restrictions may also be considered.

Technological controls such as Parental Controls, Web Filtering, Device Controls etc. should be considered. These are effective controls for setting a ‘baseline’ Internet access environment. Staff, volunteers and carers should be trained to understand the limitations and benefits of technical controls so that they can be applied appropriately and effectively.

Staff, volunteers and carers are routinely in possession of personal information relating to children and young people. Data must be processed in accordance with current data protection law; Caldecott’s policies and processes are designed to comply with fostering regulations, data protection and human rights laws. It is essential that consideration is given to all information exchanges to ensure that it is available only to people who have a need to access it. Computers and other information devices such as mobile telephones must be protected by user names and passwords/pins as the technology facilitates.

Personal information collected in relation to the child or young person may include ‘special categories’ of personal information, which is particularly sensitive. The storage, use or transfer of information must therefore be managed and protected in accordance with current data protection legislation. In the event that data is compromised, the incident must be reported via Caldecott’s Incident Reporting process which may result in regulatory reporting to the Information Commissioner’s Office.

**Monitoring**

Staff and carers will discuss the applicability of the Online Safety control environment taking the age of the child into consideration. This discussion will include carer technical competence to determine what assistance or training is required; this in order to provide the appropriate controlled environment that will best enable access to necessary Online resources whilst providing acceptable levels of protection.

The Registered Manager will be responsible for risk assessing any data breaches or failure of protocol and to ensure onward reporting to relevant authorities such as Caldecott’s Data Protection Officer, the Information Commissioners Office etc.

**Remediation**

Where access to the Internet or other communication systems is ineffectively managed, a review of training will be held.

Reportable data loss incidents will trigger a review of information processing and access controls within the Caldecott setting.