|  |  |
| --- | --- |
| Caldecott Fostering Online Safety Policy: Appendix 2: Acceptable Use Policy | Document OLS-A29thth February 2025 |
| Authorised by: |  |

**Introduction**

This Acceptable Use Policy (AUP) is in the context where a child or young person is provisioned access to the Internet or other technical communications facility in a foster home environment. Unlike standard school settings, it is likely that access is facilitated by a carer via a standard Internet Service Provider in the home for use on equipment or devices owned by a school, Local Authority, the carer or by the child or young person themselves.

The document must be read and understood by Caldecott staff, volunteers and carers. The content of the policy must be communicated to children and young people. The AUP should be used as a discussion document so that all parties understand what constitutes acceptable and reasonable use of technology in the home environment in the context of the age or maturity level of the child.

**Scope**

Where equipment or devices are provided by a school or Local Authority, separate AUP’s will be in force as is standard practice by those organisations. This AUP is limited to equipment and devices owned by the carer or the child. The core context of this AUP is that it is directed toward carer responsibilities and child behaviour.

**Guidance**

Technical and Parental controls can be effective tools for safeguarding young people in terms of Online Safety. Some tools can be subverted but they are still useful especially for protecting younger children or to prevent accidental inappropriate access.

Managing behaviour and encouraging safe Internet practice are effective and necessary strategies to complete the Online Safety safeguarding initiative.

It is strongly recommended that carers hold open and frequent discussions concerning Online Safety directly with children with emphasis on positive elements. Carers should familiarise themselves with the technical settings on connected devices as well as with the current threat landscape in relation to online safeguarding.

**Policy Statements**

1. Access to the Internet is provided to enhance education, research and social mobility. The use of swearing or intimidating language MUST NOT be used in any technical communications.
2. Users MUST NOT access, create, download, store or transmit information that is, indecent, obscene, unlawful, under copyright or that may cause offence to others.
3. Where security measures are provisioned to limit or protect technical equipment, users MUST NOT attempt to subvert or bypass security controls including using or sharing another user’s access account credentials.
4. Where technical communications such as social networks, chatrooms etc. are permitted, users SHALL report any conversations or communications that make them feel uncomfortable, threatened or otherwise adversely affected. The responsible carer SHALL onward report any such occurrences through Caldecott’s Incident Reporting mechanism.
5. The use of digital media such as video and photography MUST be controlled. It is possible that devices used for taking video or still images can append location information to digital media. Legal restrictions may persist and be relevant to specific placements. Carers MUST review recording and posting (e.g. on social media Internet sites), of digital media and consult with Caldecott staff to determine appropriate use.
6. Users MUST NOT divulge personal information about themselves without consulting Caldecott staff or carers to determine appropriateness.

**Monitoring**

Staff and carers will discuss Online Safety during the course of placement meetings where the carer will describe the adherence to the AUP by the child or young person. A record of the discussion will be retained by staff in the normal execution of their duties.

**Remediation**

Where policy is not complied with on a consistent basis, the control environment should be re-examined to determine whether strengthening those controls will provide an effective countermeasure.