

Ofsted inspectors are trained to ask how your home keeps young people safe online. Work through each item below, tick what is in place, and you will have clear evidence ready for your next inspection. Anything left unticked is a priority action.

1. Governance and accountability

- | | |
|--------------------------|---|
| ☐ | A named senior person is responsible for internet filtering and monitoring, and every staff member knows who it is. |
| ☐ | A written online safety policy exists, is reviewed at least annually, and reflects how the home actually operates. |
| ☐ | Filtering and monitoring arrangements are formally reviewed at least every three months, with the review documented and signed off. |
| ☐ | Online safety is a standing item in staff meetings and induction for new staff. |

2. Secure WiFi

- | | |
|--------------------------|--|
| ☐ | Each young person has an individual WiFi profile, so restrictions can be applied per child without affecting others. |
| ☐ | Staff use a separate, secure network that young people cannot access. |
| ☐ | Access can be limited by time of day, for example switched off overnight, per young person. |
| ☐ | WiFi passwords are managed centrally and changed when staff leave or placements end. |
| ☐ | Visitors and contractors use an isolated guest network. |

3. Filtering and monitoring

- | | |
|--------------------------|--|
| ☐ | Your filtering provider is a member of the Internet Watch Foundation and blocks illegal child abuse content. |
| ☐ | Filtering levels are appropriate to each young person's age, understanding and placement plan. |
| ☐ | Alerts are generated for concerning searches, such as references to self harm, suicide or grooming, and staff know how to respond. |
| ☐ | Filtering applies to every connection, including any backup internet line and all WiFi networks. |
| ☐ | Browsing logs are retained and can be produced as evidence of monitoring. |

4. Devices and mobile phones

- | | |
|--------------------------|--|
| ☐ | Devices owned by the home are managed through mobile device management, with app and content controls applied. |
| ☐ | Each young person's mobile phone arrangements are recorded and consistent with their placement plan and risk assessment. |
| ☐ | Gaming consoles, smart TVs and tablets are included in your filtering and WiFi controls, not just computers. |
| ☐ | There is a clear, recorded procedure for safe storage or restriction of devices where a risk assessment requires it. |

5. Data protection

- | | |
|--------------------------|---|
| ☐ | Staff email used for sensitive information about young people is encrypted. |
| ☐ | Access to records is restricted to the staff who need it, with individual logins, not shared accounts. |
| ☐ | An up to date register lists every device and IT asset in the home. |
| ☐ | Data protection arrangements comply with UK GDPR and the Data Protection Act, and staff have received training. |

6. Incidents and inspection evidence

☐	There is a written escalation process for online safety incidents, and staff can describe it.
☐	Incidents are recorded, reviewed and used to update risk assessments and filtering settings.
☐	You can show an inspector, on request: the online safety policy, the latest filtering review, alert logs and incident records.
☐	You can answer: when was filtering last reviewed, how do you know it works, and who is responsible.
☐	Lessons from incidents and reviews are shared with the whole staff team.

Not sure about some of these items?

QLine IT specialises in IT for children's homes: secure per child WiFi, internet filtering, mobile device management, encrypted email and full IT support, all designed around Ofsted and Scottish Care Inspectorate expectations. Our staff hold enhanced DBS status and we are Cyber Essentials Plus certified. Book a free, no obligation review of your home's setup.

qlineit.com/childrenshomes | 0330 1700 092

This checklist is general guidance, not legal or regulatory advice. © 2026 PC Repair Leeds Ltd, trading as QLine IT.