# Acceptable Use Policy Control Implementation Checklist

To ensure that all security policies requirements are consistently implemented, monitored, and maintained, the following checklist has been developed. It translates specific policy controls into actionable tasks, assigns clear ownership, and establishes tracking mechanisms to support ongoing compliance and operational effectiveness.

| **Policy Reference** | **Control Description** | **Frequency** | **Evidence Required** | **Status** | **Note** |
| --- | --- | --- | --- | --- | --- |
| **Acceptable Use** | Ensure all staff acknowledge the Acceptable Use policy. | Annually and during Onboarding | Acknowledgement record |  |  |
| **Acceptable Use** | Review access permissions and enforce the principle of least privilege | As needed or after all off-boarding of staff | Updated user permission |  |  |
| **Acceptable Use** | Regularly scan all devices for malware threats. | As needed | Configuration |  |  |
| **Acceptable Use** | Review white/black lists of websites of applications | As needed | Updated black/white list |  |  |
| **Acceptable Use** | Remove all identified unauthorised software from devices | As needed | Software inventory |  |  |
| **Acceptable Use** | Ensure all staff complete security awareness training | Quarterly | Acknowledgement record |  |  |