Visitors Acceptable Use Policy (AUP)

Data Security and Confidentiality

- **Protecting Information:** Visitors must not access, share, or store any confidential school, student, or staff information (including names, addresses, or photos) unless explicitly authorized and required for their duties.
- **Password Security:** If provided a guest account, visitors must keep their login credentials private and log out immediately after use, especially on shared devices.
- **Device Security:** Any personal device connected to the school's network (if permitted) must have up-to-date anti-virus protection to prevent introducing malware.

Use of Technology and Network Access

- **Purpose of Access:** Any access to the school network (Wi-Fi, computers, printers) is strictly for the purpose of the visit or agreed-upon duties.
- **Filtering and Monitoring:** Visitors must understand and agree that the school's systems are monitored and filtered for safety and security. They must **not** attempt to bypass any security systems, firewalls, or internet filters.
- **Unauthorised Activity:** Prohibited actions include:
    - Downloading or installing unauthorized software.
    - Attempting to access restricted areas of the network.
    - Causing intentional damage or disruption to the school's IT equipment or network.
- **Appropriate Content:** Visitors must not access, download, or share any material that is illegal, offensive, obscene, or otherwise inappropriate for an educational setting (e.g., hate speech, extremist material, or pornography).

Photography and Digital Media

This is often the most critical safeguarding point for visitors:

- **No Unauthorised Images:** Visitors are **strictly prohibited** from taking photographs or video footage of students or staff using any personal device (e.g., mobile phone, camera) without the express permission of a senior member of staff and, where applicable, the subjects themselves.
- **Media Sharing:** Any images or information obtained during the visit must not be published or shared online (e.g., social media, blogs) without explicit, written school permission.

Mobile Devices and Personal Communication

- **Minimizing Distraction:** Personal mobile phones should generally be kept on silent or vibrate and use kept to a minimum, especially when unsupervised around students.
- **Professional Boundaries:** Visitors must only communicate with students or parents via official, school-approved channels. Sharing personal contact information (email, phone number, social media handles) with students or parents is generally forbidden.

5. Reporting and Consequences

- **Duty to Report:** Any accidental access to inappropriate content, a security issue, or a suspected breach of the policy must be immediately reported to a member of staff (often the designated safeguarding lead or IT manager).
- **Consequences of Misuse:** Failure to comply with the AUP may result in the immediate loss of access to school systems, removal from the school premises, and potential disciplinary or legal action.

Name: **Signature:**

Role: **Date:**