Regular Visitor Acceptable Use Policy

Visitors will

- apply appropriate standards when using computing devices in school including an awareness of Data Protection, Copyright laws, Prevent duty and reporting.
- only use personal devices, including a mobile phone during the working day in line with the policy for use by staff. This includes not using the device in the presence of child and not taking pictures or other recordings unless permission has been granted. The device must be pin code or fingerprint protected and not discoverable by third parties.
- not publish any information online that may be offensive to staff or pupils, or may bring the school into disrepute.

Logging in

- If you use the school's equipment, then request a guest log in.
- If you are using equipment that has been logged in by a member of staff they will always ensure they are in the room with you. They will lock the machine if they need to leave the room.
- If your service contract (Network/MIS support) allows you access to the system through team logins, inform the school of the purpose and how you will be accessing the system.

Internet Access and uploading

- The school's internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the schools normal filtering system. This might not be possible as changes to the filter can take some time.
- You are responsible for the sites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never upload and install software or updates without permission from a member of staff.

If you use your own equipment:

- Make sure that you have permission from the school for its use
- Ensure it has up to date virus protection software installed.
- Ensure that you take appropriate precautions with trailing wires.
- Ensure that you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.

Wireless Access

- Where you have permission to use a personal smart device, you will use the school's wireless connection and will be provided with an authorisation key.
- Remember that bandwidth is limited so avoid intensive use such as large downloads.

Downloading / Transferring files or documents

For all files

- Never transfer files unless you have permission, this must not be from a USB stick/external drive unless permission has been given by the headteacher.
- Make sure that you clearly state the purpose for transferring the files.

If the file contains sensitive personal data such as staff or student information

- Get permission for this in writing or by email.

(Note: permission will not be needed where existing service contracts, such as Network/MIS support, are in place. However, please indicate the type of work you will be doing).

- Transfer the file only over a secure email connection.

If you need to take pictures, video or record sound files then check that

- you have permission to capture these files.
- the staff/children have all given their permission for these images/voices to be used.
- you request permission in writing or through email should you intend to use these files in a public arena (website, blog etc.) or for financial gain.

Reporting

- Report any incidence of accidental viewing of inappropriate images or materials.
- Report any incidence of deliberate searching for inappropriate images or materials.
- Switch off and secure any device that you suspect of containing an intimate sexting image and report immediately to the school's safeguarding lead.

Name _____ Date _____