Governors Acceptable Use Policy (AUP)

Data Confidentiality & Security

- **Handling School Data:** Governors must **not** store sensitive school data (e.g., meeting minutes, pupil data, finance reports) on personal devices (laptops, phones, USB drives) unless the devices are **encrypted** and password-protected to a strong standard.
- **No Sharing:** Passwords, login credentials for school portals, or confidential documents must never be shared with anyone, including family members.
- **Logging Out:** Governors must **lock their screen or log out** of any school system (e.g., GovernorHub, school email) immediately when leaving a device unattended.
- **Reporting:** The loss, theft, or suspected compromise of any device or school data must be **immediately reported** to the Headteacher or Data Protection Officer (DPO).

Professional Communications

Communication must always maintain professional boundaries and transparency.

- **Official Channels Only:** Governors must only use **official school email accounts** or approved, secure governance platforms for all school-related business, particularly when discussing confidential matters. Personal email accounts should not be used for school business.
- **Pupil Contact:** Direct, one-to-one communication with students (via email, social media, or phone) is **strictly prohibited** unless explicitly approved and monitored by the Headteacher for an agreed-upon, professional purpose (e.g., a specific curriculum link role).
- **Professional Tone:** All communications must be professional, respectful, and transparent, reflecting the school's values.

Internet Use and Social Media

Governors are seen as role models and their online conduct is subject to scrutiny, both on and off-site.

- **No Bypass:** Governors must **not attempt to bypass** the school's security, monitoring, or internet filtering systems when using school equipment or the school network.
- **Appropriate Content:** School systems, networks, and personal devices used to access school information must **never** be used to access, download, or distribute material that is illegal, discriminatory, offensive, or otherwise inappropriate for an educational setting.
- **Online Reputation:** Governors must ensure their **personal use of social media** (including private accounts) does not bring the school or its staff/students into **disrepute** by posting negative, threatening, or sensitive comments about the school community, policies, or incidents.

Use of Mobile Devices and Images

This is crucial for safeguarding and maintaining professional boundaries while on site.

- **Device Use in School:** Personal mobile phones should generally be on **silent or switched off** during meetings, lessons, or in areas where children are present, and their use should be minimised.
- **Photography/Recording:** Governors are **prohibited** from taking photographs, videos, or audio recordings of pupils, staff, or the school site using any personal device without the express, prior permission of the Headteacher. Any approved images must be handled in line with the school's data protection policy.

    To be completed by the Headteacher to issue access/usage permissions
    I approve this user to be allocated credentials for school systems as relevant to their role.
- **Systems: Arbor, LGFL Staff mail, Server network, Smartlog, Governor Hub**

Signature: Signature:

Name: Joe Porter   Name:
Date: Date: