



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



Staff Acceptable Use Agreement

The Bluebell Federation: Rooted and Established in Love. |

Our Bluebell Federation Vision: Every child will blossom academically and emotionally in a nurturing environment rooted in love and kindness. |

This policy was adopted in October 2026

This policy is due for review in September 2027



Professional use of technology

As a member of staff, I agree that I will:

- use technology in a way that supports safeguarding, teaching, learning, administration and the professional responsibilities of my role;
- use only accounts, systems, applications, AI tools and devices that are authorised for the work I am carrying out;
- follow the Staff Behaviour / Code of Conduct, Core Online Safety Policy and relevant supporting procedures when using technology on or off site;
- maintain professional boundaries in all electronic communication with pupils, learners, parents and carers;
- only use organisational accounts and approved communication systems for setting business and not use personal email, personal phone numbers, personal messaging accounts or personal social-media accounts for contact with pupils or parents/carers;
- declare any unavoidable pre-existing personal, family or community relationship that could conflict with these boundaries so that it can be managed appropriately;
- not accept or initiate personal social-media contact with current pupils or learners or any children of school or college age arising from the professional role; unavoidable pre-existing family/ social/ community relationships must be declared and managed;
- not use personal social media for any communications with parents/carers;
- report personal-channel contact from a pupil or parent where it creates a safeguarding or professional-boundary concern.

Accounts, devices and cyber security

- keep passwords, passphrases, authentication codes and other security credentials private;
- use multi-factor authentication where required and never approve an

- unexpected authentication request;
- lock or log out of devices when appropriate and take reasonable care of setting-owned equipment;
- report suspicious messages, phishing, unusual device behaviour, lost or stolen devices, compromised accounts and other cyber concerns promptly;
- not deliberately bypass filtering, monitoring, device-management, network or security controls;
- not install unauthorised software, browser extensions or applications on managed devices;
- not use personal mobile data, hotspots, VPNs or other workarounds to avoid setting security or filtering controls;
- use setting-owned or approved devices for work wherever required by local arrangements.

Personal devices, images and recording

- not use my personal phone, smart glasses, wearable camera or other personal device to photograph, film or record children, except under a formally authorised exceptional arrangement;
- not use personal devices to store safeguarding records, confidential pupil information or other setting data outside approved arrangements;
- use personal devices only in accordance with the Mobile Phone and Personal Device Policy and in ways that do not interfere with my duties or undermine the expectations applied to pupils;
- not use smart watches, smart glasses or AI-enabled wearables to capture, transcribe, summarise or transmit confidential conversations or safeguarding information.

AI and emerging technology

- use AI only for legitimate, approved educational or organisational purposes in accordance with the AI and Emerging Technology Procedure;

Staff Acceptable Use Agreement

- not enter personal, confidential, special category, safeguarding, medical or sensitive information into an AI tool unless the use has been explicitly approved and the relevant data-protection controls are in place;
- critically check AI output for accuracy, bias, fabricated information, harmful content and appropriateness before I use or share it;
- remain personally and professionally responsible for safeguarding, assessment, disciplinary and other high-impact decisions and not delegate those decisions to AI;
- not use AI to impersonate another person, create deceptive communications, generate sexualised content, or produce harmful deepfakes or cloned media;
- follow approved-use, copyright, intellectual-property, assessment and transparency requirements when using AI-generated content;
- report harmful AI output, privacy incidents or AI-related safeguarding concerns through the appropriate route.

Safeguarding, privacy and professional conduct

- report online-safety and safeguarding concerns promptly to the DSL or safeguarding team and not assume a technical alert will identify every concern;
- not conduct my own investigation into harmful or sexual content where the Incident Response Procedure requires DSL-led action;
- not create, request, unnecessarily view, copy, print, save, share or forward nude, semi-nude or sexual imagery involving children;
- protect personal and confidential information and use approved methods when sharing sensitive information;
- respect copyright, licensing and intellectual-property requirements;
- ensure my personal online activity remains compatible with my professional responsibilities and does not disclose confidential setting information or

Staff Acceptable Use Agreement

misrepresent personal views as the setting's position;

- raise concerns if a policy, technical control or approved tool creates a safeguarding, accessibility or operational problem.

Monitoring and accountability

I understand that use of organisational systems, accounts and managed devices may be filtered, monitored or logged for safeguarding, security and operational purposes in accordance with the setting's policies and privacy arrangements.

I understand that breaches of this agreement may be managed under the Staff Behaviour / Code of Conduct, safeguarding, disciplinary, data-protection, cyber-security or other relevant procedures.

Acknowledgement

Staff member name	[Insert]
Role	[Insert]
Signature / acknowledgement	[Insert]
Date	[Insert]