Best Foot Forward - Online Safety Policy

Author: Andrew Russell
Approved By: Bethany Russell
Date Approved: October 2025
Assigned Review Period: 1 Year
Last Reviewed: 14 October 2026
Next Review Due: October 2027

This policy applies to BFF leaders, employees, self-employed practitioners, contractors, volunteers and learners during BFF work in homes, schools, community venues and online. It also covers online conduct outside sessions that raises safeguarding or professional-boundary concerns. Read it with the policies in Section 1.

Statement of Intent

Best Foot Forward (BFF) uses digital services to support learning and communication within non-school, one-to-one alternative provision. Safe use requires suitable accounts, checked resources, supervision and effective technical controls where available. BFF must confirm the protections in each setting rather than assume that a school, home Wi-Fi connection or mobile hotspot provides BFF filtering and monitoring.
The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- Content: Being exposed to illegal, inappropriate, or harmful material (e.g., pornography, fake news, self-harm and suicide, discriminatory or extremist views).
- Contact: Being subjected to harmful online interaction with other users (e.g., peer pressure, commercial advertising, adults posing as children or young adults with the intention to groom or exploit children).
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm (e.g., sending and receiving explicit messages and cyberbullying).
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Assess these risks for the learner, activity, device, accounts and connection actually used. Include SEND, communication and emotional needs without assuming vulnerability means inability. Take account of harm through gaming, messaging, livestreams, AI tools and offline device sharing as well as websites. Pause an activity if essential safety controls are missing.

1. Legal Framework

Apply relevant legal duties and current guidance. KCSIE and DfE school standards inform BFF practice and commissioner arrangements; school-specific duties and powers do not automatically apply to non-school provision. Sources include:

- Voyeurism (Offences) Act 2019

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE current filtering and monitoring core standard for schools and colleges, used as a benchmark for actual BFF arrangements
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE Keeping Children Safe in Education 2026; Working Together to Safeguard Children 2026; non-school AP voluntary national standards
- DfE Teaching online safety in school and current statutory RSHE guidance, effective September 2026
- Equality Act 2010; relevant safeguarding law, including Care Act 2014/Mental Capacity Act 2005 for adults at risk. School Searching, screening and confiscation guidance does not give BFF compulsory search powers.
- DfE current Generative artificial intelligence in education and relevant AI/data-protection guidance
- UKCIS Sharing nudes and semi-nudes: advice for education settings, updated March 2024, including digitally manipulated and AI-generated imagery
- UKCIS (2020) 'Education for a Connected World'
- Current NCSC small-business, password and account-security guidance

This policy operates alongside the following Best Foot Forward policies:

- Social Media Policy
- Managing Allegations; Low-Level Concerns; Safeguarding Governance Summary; Governance and Accountability Framework
- ICT, Internet Acceptable Use and Social Media Policy and approved user agreements
- Cyber-security and incident response arrangements; Business Continuity Policy
- Risk Assessment and Lone Working policies
- Child Protection and Safeguarding Policy
- Child-on-child Abuse; Safeguarding Adults Procedures
- Anti-Bullying Policy
- Student and Staff Electronic Devices Policy
- Staff Code of Conduct
- Behaviour and Positive Relationships Policy
- Applicable disciplinary/engagement procedures, reflecting actual status and contractual arrangements
- Data Protection; SAR; Data Retention and Disposal policies
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Professional Boundaries and Communication Policy
- Prevent Duty Policy
- Remote Education; Remote and Virtual Meetings policies

2. Roles and Responsibilities

The CEOs retain organisational accountability and will be responsible for:

- Ensuring lawful, proportionate arrangements for BFF's actual provision, with evidence of implementation rather than a claim that a policy alone guarantees safety.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, during induction and at regular intervals.
- Documenting the actual filtering/monitoring coverage, gaps and safeguards in each delivery setting; reviewing effectiveness at least annually and after incidents or material changes with competent technical support.
- Assigning named responsibilities for technical controls, reports/alerts, response times and absence cover, and ensuring staff understand how to escalate concerns.
- Ensuring policies include an effective approach to planning for, and responding to, online challenges and hoaxes.

Appointed operational leads, within recorded delegated duties, will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout policies and procedures, including those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and other relevant staff by ensuring they have enough time and resources to carry out their responsibilities.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Auditing and evaluating online safety practices.
- Engaging with parents to keep them up to date with current online safety issues and Best Foot Forward's approach.
- Completing half-termly checks of incidents, actions and changed risks with the DSL and competent technical support where needed; supporting the annual full review.

The DSL (Bethany Russell), supported by Deputy DSL Andrew Russell and agreed delegated support from Kathie Sweeney, will be responsible for:

- Taking the lead responsibility for online safety.
- Undertaking training to understand the risks associated with online safety, including additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters (e.g., Tutors, Mentors and IT suppliers).
- Ensuring online safety is recognised as part of safeguarding responsibilities and that a coordinated approach is implemented, including for remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use by students and staff, and ensuring all members of the community understand this procedure.
- Understanding the filtering and monitoring processes in place and ensuring safeguarding training includes related expectations, roles and responsibilities.
- Maintaining records of reported online safety concerns and actions taken.

- Monitoring online safety incidents to identify trends and gaps, and using data to update procedures.
- Providing a restricted termly online-safety assurance summary to the CEOs, with actions, owners and deadlines. Leadership concerns require independent routes under the Governance Summary.
- Working with CEOs and relevant technical support on half-termly checks and the annual review; safeguarding advice is distinct from specialist technical competence.

The CEO-appointed competent technical contact/support provider, working with the DSL, will be responsible for:

- Providing technical advice and configuration within the agreed remit; a standing IT supplier or a BFF-controlled network must not be assumed.
- Implementing appropriate security measures as directed by the CEO.
- Ensuring that filtering and monitoring systems are updated as appropriate.
- Supporting documented checks, reviews and incident response; report failures promptly and distinguish technical alerts from safeguarding decisions.

All staff members will be responsible for:

- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Modelling safe use and maintaining professional boundaries through approved work accounts/channels. Personal-device approval does not authorise private-account contact or learner images in personal galleries.
- Maintaining awareness of online safety issues and indicators that students may be unsafe online.
- Taking immediate protective action and reporting concerns promptly to the DSL/deputy, including where harm occurs outside sessions or BFF systems. Notify the DPO/CEO of suspected data or account compromise.
- Embedding online safety within the curriculum where relevant to their role.

Learners will be supported accessibly to:

- Understand and follow agreed safe-use arrangements with reasonable adjustments and support. An unsigned agreement does not prevent access to safeguarding help.
- Seek help from staff if concerned about something they or a peer have experienced online.
- Report online safety incidents and concerns through accessible agreed routes.

3. Managing Online Safety

Online safety forms part of safeguarding, learner support and information security. The DSL leads the safeguarding response; CEOs retain accountability and assign competent technical assistance. This policy does not authorise routine access to private devices, accounts, messages or passwords.

The DSL seeks police/social care advice and makes referrals where required for online abuse or exploitation. For adults at risk, use adult safeguarding procedures. Any staff member may refer directly where necessary; do not wait for internal permission or a particular lead.

Online safety is integrated across Best Foot Forward operations in the following ways:

- Staff receive regular training.

- Staff receive regular email updates regarding online safety information and any changes to guidance or legislation.
- The CEO actively supports the DSL with this policy and its implementation.
- Online safety is integrated into learning throughout the curriculum.
- Information, advice and guidance are provided for parents/carers.

Handling Online Safety Concerns

- Disclosures made by students about online abuse, harassment, or exploitation will be handled in line with the Child Protection and Safeguarding Policy.
- Staff recognise harmful online sexual behaviour can progress on a continuum; early intervention is essential.
- Listen calmly, support the learner and consider their wishes, age, needs and ongoing risk. Inform parents/carers where appropriate and safe; do not notify automatically if this could increase risk or prejudice enquiries. Record decisions and seek statutory advice where needed.
- Do not promise secrecy. Share necessary safeguarding information lawfully, proportionately and securely, recording the basis and reasons. Consent is not always required; do not assume BFF can rely on public task merely because it is commissioned by a school or local authority.
- Staff concerns go to an unimplicated authorised handler under allegations/low-level-concerns procedures. Concerns about either CEO, both leaders or their handling use an independent unconflicted adviser and/or relevant LADO/statutory services directly; Andrew and Bethany are not independent reviewers of each other.
- The DSL assesses risk, coordinates support and obtains appropriate advice/referrals. Tutors must not investigate privately, confront suspected perpetrators or demand access to accounts. Do not conduct substantive internal enquiries that could prejudice police/social care or LADO processes.
- Respond proportionately, without blaming or unnecessarily criminalising a child. Staff must report promptly; the DSL seeks police/social care advice where required, rather than treating every online incident as an automatic police matter.
- Record factual concerns, learner words, immediate action, referrals and follow-up securely. Child safeguarding goes to CPOMS; routine progress/attendance to DCPro. Staff allegations remain restricted. Preserve necessary records for active enquiries, complaints, SARs and legal holds.

If no lead is available or there is immediate danger, contact the appropriate social care/police service directly and call 999 where necessary. LADO routes concern allegations about adults working with children; they do not replace a referral for a child's safety. Use current contacts in the Governance Summary and record receipt/follow-up.

4. Cyberbullying

Cyberbullying can include, but is not limited to:

- Threatening, intimidating, or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others.

- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites, and social networking sites.
- Abuse between young people in intimate relationships online (teenage relationship abuse).
- Discriminatory bullying online (e.g., homophobia, racism, misogyny/misandry).

Some learners face additional online targeting or barriers to seeking help, including those with SEND or protected characteristics. Assess individual circumstances, including whether the person targeted or causing harm needs safeguarding support. Use the Anti-Bullying and Behaviour policies; never require a forced apology, disclosure or joint meeting with an alleged perpetrator.

5. Child-on-Child Sexual Abuse and Harassment

Abuse may occur inside or outside sessions, online or offline. Shame, fear or coercion may prevent disclosure; respond supportively regardless of the service used and do not treat visiting an unsuitable website as making a learner responsible for abuse.
Examples of harmful online sexual behaviour include:

- Threatening, facilitating or encouraging sexual violence.
- Upskirting (taking a picture underneath a person's clothing without consent).
- Sexualised online bullying (e.g., sexual jokes or taunts).
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online.

Sexual harassment and abuse must never be dismissed as banter. Sexual imagery involving under-18s raises serious safeguarding and legal issues, including when shared with apparent agreement or generated/manipulated by AI. Follow Child-on-child Abuse, safeguarding and UKCIS procedures; protect and support children without shaming them.

Never request, intentionally view, screenshot, download, copy, print, forward or upload child nudes/semi-nudes, including suspected AI imagery. If encountered accidentally, stop viewing, reassure the learner and tell the DSL promptly. Record necessary non-image details; do not attach imagery to CPOMS or ask a learner to show it as proof. Follow DSL/police advice on devices, evidence, deletion and reporting.

For sextortion, coercion, adult involvement or immediate risk, seek urgent police/social care advice under safeguarding procedures. Do not negotiate with an offender, encourage payment or send further imagery. Any exceptional DSL viewing decision must follow full UKCIS guidance, be necessary for safeguarding and recorded; it is not authority for ordinary staff to investigate images.

6. Grooming and Exploitation

Grooming involves building a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them. Staff will be trained to recognise indicators of grooming and online abuse.
Indicators may include:

- Being secretive about time spent online.
- Having an older boyfriend or girlfriend unknown to close friends.
- Unexplained money or new possessions (e.g., clothes, devices).

Child sexual exploitation (CSE) and child criminal exploitation (CCE):

- CSE may include online coercion and involvement in wider exploitation.
- CCE can involve manipulation into committing crimes; recruitment and manipulation increasingly occur online.
- Report concerns promptly to the DSL/deputy and take necessary protective action. Indicators are not proof and absence of indicators does not show safety. Apparent cooperation does not remove the possibility of coercion, abuse or exploitation.

Radicalisation:

- Staff will be vigilant to indicators of radicalisation and online grooming by extremists.
- Concerns will be reported to the DSL and handled in line with the Prevent Duty Policy.

7. Mental Health

Online activity may support or harm wellbeing. Be alert to self-harm/suicide content, eating-disorder material, isolation, compulsive use and distress, including dependency on AI companions. Tutors do not diagnose or provide crisis treatment outside competence. Follow learner plans and safeguarding procedures; immediate risk requires urgent protective action and emergency help where necessary.

8. Online Hoaxes and Harmful Online Challenges

An online hoax is a deliberate lie designed to seem truthful, often intended to scaremonger. Harmful online challenges may put participants at risk directly or via online distribution. Report concerns to the DSL without deliberately seeking out or sharing harmful material. Assess credible risk and respond accessibly and proportionately; avoid circulating challenge names, instructions or graphic content that could amplify harm. Use checked resources and current agency advice.

9. Cyber-Crime

Cyber-crime categories include:

- Cyber-enabled crimes (e.g., fraud, sale of illegal drugs, sexual abuse/exploitation).
- Cyber-dependent crimes (e.g., malware, illegal hacking, 'booting'/DDoS).

The DSL may consider referral to the Cyber Choices programme where appropriate. Students are taught to use technology safely, responsibly and lawfully.

10. Online Safety Training for Staff

Provide safeguarding/online-safety induction before work, updates at least annually and further instruction as risks change. Cover the 4Cs, SEND, exploitation, sexual imagery, AI, approved contact/recording, actual filtering/monitoring limits, alerts and emergency reporting. Record training and check understanding; assigned specialists need suitable competence.

11. Online Safety and the Curriculum

Online safety is embedded throughout the curriculum, particularly within:

- RSHE
- PSHE
- Digital Skills

Teaching is age- and development-appropriate, adapted to SEND, communication and lived experience. Include source checking, misinformation/deepfakes, privacy, consent and coercion, reporting, digital footprints, scams and purchases. Use supportive language and safe examples; do not require personal disclosures or use graphic sexual/self-harm material. The DSL contributes to curriculum development and tailoring for vulnerable cohorts (e.g., SEND, LAC). External resources and visitors are reviewed for suitability. Sessions are planned to avoid highlighting individuals who may be affected and to maintain a safe environment for discussion.

12. Use of Technology during Sessions

Technology used during sessions may include:

- Laptops
- Tablets
- Internet
- Email
- Cameras

Before use, check websites, apps and resources for suitability, privacy, copyright and current age/account terms; parental permission does not override platform restrictions. Use approved staff work accounts and supervise actual learner use. Do not assume a checked link remains safe after redirects, adverts, chat or content changes.

13. Use of Smart Technology

Students will be educated on acceptable use of personal devices in line with the ICT Acceptable Use Agreement. Staff will follow the ICT Acceptable Use Policy.
Inappropriate use may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Learner device use follows the agreed plan and Electronic Devices Policy, including accessibility, health and communication needs. Explain restrictions and safe alternatives; respond proportionately to misuse without removing essential support or ending supervision unsafely. Tutors have no general power to search devices, demand passwords, read private messages or forcibly confiscate items.

14. Educating Parents

Share relevant safe-use arrangements at induction/referral and when they change, and provide timely accessible information about current risks. Agree supervision, approved communication and online session support with families/commissioners. Partnership does not transfer BFF's safeguarding duties to parents.
Parents are made aware of risks including:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing nudes/semi-nudes, sextortion and manipulated/AI-generated sexual imagery
- Cyberbullying.
- Exposure to age-inappropriate or harmful content.

Awareness is raised via:

- Direct communication from staff.
- Newsletters.
- Online resources.
- Handover conversations with Tutors/Mentors.
- Input during Annual Review and other multi-agency meetings.

15. Filtering and Monitoring Online Activity

CEOs, DSL and competent technical support must document which devices, accounts, services and connections are covered by filtering and monitoring, their limits, and safe alternatives for gaps. Use current DfE standards as a benchmark; do not claim full coverage of homes, venue Wi-Fi, personal devices, hotspots or mobile data without evidence.

Record approved filtering changes, reasons and risk assessment; assess both harmful access and excessive blocking of legitimate learning. Assign who reviews reports/alerts, how often, response times and absence cover. Review effectiveness at least annually, with risk-based checks and reviews after incidents or changes, including AI-generated/live content.

Monitoring must be lawful, necessary, proportionate and transparent. Explain actual work-system monitoring, its purpose, access and retention; no routine inspection of private accounts or blanket waiver of privacy. Active supervision remains necessary. If harmful content, bypassing or failed controls arise, stop the affected activity, use a safe alternative and report promptly. Do not promise continuous monitoring unless provided.

16. Network Security

Keep approved devices, applications, malware protection, backups and security settings current through assigned competent support. Report loss, compromise or suspicious attachments immediately to management/DPO and the DSL if learner safety is affected. Follow containment and evidence-preservation advice; do not improvise recovery or delete evidence.
Use individual authorised accounts, strong unique passwords/passphrases and approved secure recovery arrangements; use MFA or suitable passkeys where supported. Keep credentials private and lock unattended devices. Change passwords promptly on suspected compromise or incident instructions; do not require routine expiry without a security reason. Staff must not ask learners for private passwords.

17. Emails

Use BFF-approved professional accounts/channels for work and learner/family contact, under ICT and Professional Boundaries policies. Approved secure personal devices may host work accounts; private email, personal numbers and social accounts are not work contact routes. Families/learners may use suitable own accounts or approved guest access.
Share only necessary information through approved secure routes, checking recipients and permissions. For sensitive records, use protected sharing/encryption as appropriate; a standard email or recall does not guarantee safety. Do not click suspicious links or attachments; report through the approved route and preserve relevant evidence rather than deleting it independently.
Phishing awareness includes:

- Checking sender legitimacy.
- Recognising suspicious domains and display names.
- Being cautious of urgent calls to action.
- Checking spelling and grammar anomalies.

Suspected cyber incidents require immediate reporting and containment under current management/DPO instructions and Business Continuity arrangements. Do not wait for a future plan to be completed. Management must record response/cover, backup and recovery responsibilities and test arrangements proportionately.

18. Generative Artificial Intelligence (AI)

AI use requires CEO approval with DSL/DPO assessment of safeguarding, privacy, age requirements, supplier data use/training, security and retention. Do not enter personal, SEND, safeguarding or confidential information into unapproved tools, including indirectly identifying details. Use approved accounts, suitable supervision and necessary lawful controls; filtering cannot guarantee that unsafe outputs or data entry are prevented.
Assess AI outputs for accuracy, bias, manipulation, harmful content and copyright. AI must not make sole safeguarding or other significant decisions about learners. Do not create sexualised child imagery, impersonate people or upload images without lawful approval. Explain AI limits, unreliable advice and how learners can seek human support.

AI meeting assistants, automatic transcripts and summaries are subject to the same approval and privacy checks as recordings under the ICT and Remote/Virtual Meetings policies. Disable unapproved capture/bots. Live accessibility tools must be assessed for any stored transcript or external data sharing.

19. Social Networking

Use of social media by staff and students is managed in line with the Social Media Policy.

20. The Best Foot Forward Website

CEOs approve accurate, current website content and applicable legal/privacy information. Do not make unsupported claims about regulation, approvals, qualifications or outcomes. Learner images, work or testimonials need an approved purpose, lawful arrangements and specific permissions where appropriate, respecting learner wishes.

21. Use of Devices

BFF-owned devices are used under approved agreements; secure personal-device use requires prior approval and the Electronic Devices/ICT controls. Keep work records within approved systems, prevent household access and personal cloud/gallery backups, and report loss/unauthorised disclosure promptly.

22. Remote Learning

Apply Remote Education, Remote and Virtual Meetings and Professional Boundaries policies. Agree timing, access, learner location, emergency contact, responsible adult/support availability and connection-loss response. Use controlled entry and approved work channels. Under-18 home sessions require the agreed responsible adult present and available; do not default to personal calls or chats.
Recording, photography and screenshots are not routine. An exceptional proposal needs CEO/DPO approval, DSL input for children, a necessary purpose and lawful basis, appropriate privacy information/permissions, restricted storage and retention. Attendance or policy acceptance is not blanket consent. Respect learner wishes and agree a safe alternative where required.

23. Monitoring and Review

CEOs and DSL complete half-termly checks of incidents, changed risks and overdue actions, with competent technical input where needed; review the full policy and filtering/monitoring arrangements at least annually and after significant changes/incidents. Record evidence, owners and deadlines, verify action and brief staff. October 2027 is the proposed next review.

Appendix A: Online Harms and Risks – Curriculum Coverage

This appendix maps the '4Cs' risk framework to curriculum coverage and supporting resources. Tutors/Mentors should adapt details to cohort needs and update resources regularly.

Example coverage:

- Content: Media literacy, misinformation, age-appropriate content; covered in RSHE/PSHE/Digital Skills.
- Contact: Grooming awareness, reporting mechanisms, privacy settings; covered in RSHE and safeguarding inputs.
- Conduct: Privacy, digital footprints, respectful contact and cyberbullying responses; covered in PSHE and one-to-one learning/mentoring.
- Commerce: Advertising literacy, scams/phishing, in-app purchases and gaming/gambling risks; covered in Digital Skills and PSHE.

Bethany Russell 07394 950803
beth@bestfootforward.org.uk

Andrew Russell 07538 719783
andrew@bestfootforward.org.uk

Website: www.bestfootforward.org.uk
Contact:admin@bestfootforward.org.uk