Best Foot Forward - Online Safety Policy

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

This policy sets out Best Foot Forward's approach to online safety and should be read alongside the policies listed in Section 1.

Statement of Intent

Best Foot Forward understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout Best Foot Forward; therefore, there are a number of controls in place to ensure the safety of students and staff.
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.

The measures implemented to protect students and staff revolve around these areas of risk. This policy aims to ensure appropriate and safe use of the internet and other digital technology devices by all students and staff.

1. Legal Framework

This policy has due regard to relevant legislation and guidance including, but not limited to:

- Voyeurism (Offences) Act 2019
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education'
- DfE (2023) 'Teaching online safety in school'

- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- DCMS & UKCIS (2020) 'Sharing nudes and semi-nudes: advice for education settings'
- UKCIS (2020) 'Education for a Connected World'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates alongside the following Best Foot Forward policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- ICT Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan (under review as at Oct 2023)
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Students' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour and Positive Relationships Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy

2. Roles and Responsibilities

The Best Foot Forward CEO will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- 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.
- Ensuring that there are appropriate filtering and monitoring systems in place and that their effectiveness is reviewed at least annually with IT suppliers.
- Ensuring that the Senior Leadership Team and other relevant staff understand and can manage the filtering and monitoring systems, and know how to escalate concerns.
- Ensuring policies include an effective approach to planning for, and responding to, online challenges and hoaxes.

The Senior Leadership Team (SLT) 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.
- Working with the DSL and IT suppliers to conduct half-termly light-touch reviews of this policy and update it annually.

The Designated Safeguarding Lead (DSL) 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.
- Reporting, alongside the proprietors, on online safety on a termly basis.
- Working with the CEO, SLT, and IT suppliers to conduct half-termly light-touch reviews and to update this policy annually.

The DSL alongside the IT supplier(s) will be responsible for:

- Providing technical support in the development and implementation of online safety policies and procedures.
- Implementing appropriate security measures as directed by the CEO.
- Ensuring that filtering and monitoring systems are updated as appropriate.
- Working with the DSL and SLT to conduct half-termly light-touch reviews of this policy.

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 good online behaviours and maintaining a professional level of conduct in personal use of technology.
- Maintaining awareness of online safety issues and indicators that students may be unsafe online.
- Reporting concerns in line with Best Foot Forward's reporting procedure.
- Embedding online safety within the curriculum where relevant to their role.

Students will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from staff if concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with this policy.

3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and well-being issues affecting young people. The DSL has overall responsibility for Best Foot Forward's approach to online safety, supported by relevant staff, IT suppliers and the CEO. The DSL will liaise with the police or children's social care services for support in responding to harmful online sexual behaviour.

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.
- The DSL balances victims' wishes with the duty to protect them and other young people, and will meet with parents to discuss safeguarding measures.
- Confidentiality will not be promised; information may be shared lawfully under UK GDPR when necessary (e.g., public task).
- Concerns regarding staff online behaviour are reported to the CEO; if about the CEO, refer to the Whistleblowing Policy.

- Concerns regarding a student's online behaviour are reported to the DSL, who investigates and manages in accordance with relevant policies; illegal activity will be referred to the police.
- Best Foot Forward avoids unnecessarily criminalising students where behaviour is inadvertent; the DSL will determine appropriate responses.
- All online safety incidents and responses are recorded by the DSL.

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).

Certain students can be more at risk of abuse and/or bullying online, such as LGBTQ+ students and students with SEND. Cyberbullying against students or staff is not tolerated and incidents are dealt with in line with the Anti-Bullying Policy.

5. Child-on-Child Sexual Abuse and Harassment

Staff understand that abuse can occur both in and outside of sessions, off and online, and that students are less likely to report concerning behaviours when using inappropriate websites.

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.

There is a zero-tolerance approach to sexually harassing or abusive behaviour. Creating, possessing, and distributing indecent imagery of individuals under 18 is a criminal offence. Concerns will be managed in line with the Child-on-child Abuse Policy, Social Media Policy, and the Child Protection and Safeguarding Policy.

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.
- Concerns will be reported to the DSL without delay and managed in line with the Child Protection and Safeguarding Policy.

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 can impact a student's mental health both positively and negatively. Staff will receive training on platforms, terminology, and indicators of mental health challenges. Concerns will be managed in line with the SEMH Policy.

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. The DSL will assess any reported harmful content and determine appropriate responses that are proportionate, age-appropriate, and supportive, avoiding unnecessary amplification.

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

Safeguarding training for staff includes online safety, how the internet can facilitate abuse and exploitation, and understanding expectations relating to filtering and monitoring systems.

11. Online Safety and the Curriculum

Online safety is embedded throughout the curriculum, particularly within:

- RSHE
- PSHE
- Digital Skills

Teaching is age-appropriate and covers underpinning knowledge and behaviours, including how to evaluate online content, recognise persuasion techniques, acceptable behaviour, identify risks, and seek support.
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

Tutors/Mentors will evaluate websites, tools and apps before use and ensure materials are used in line with copyright law. Students will be appropriately supervised when using online materials.

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.

Students may not use smart devices or other personal technology during sessions unless explicitly permitted by the Tutor or Mentor. Significant misuse will be addressed in line with the Behaviour and Positive Relationships Policy.

14. Educating Parents

Best Foot Forward works in partnership with parents/carers. Parents receive information about the organisation's approach to online safety and their role in protecting their children. The IT Acceptable Use Agreement is shared annually.
Parents are made aware of risks including:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing indecent imagery (e.g., sexting).
- 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

The CEO will ensure appropriate filtering and monitoring systems are in place and meet DfE standards, avoiding unreasonable over-blocking. Roles and responsibilities for managing these systems will be clearly assigned.
Requests to change filtering are directed to the CEO. Risk assessments are conducted before changes; actions are recorded by the DSL. Deliberate breaches are escalated and addressed under relevant policies. Illegal content will be reported to appropriate agencies (e.g., IWF, CEOP, police).
Best Foot Forward's network and devices are monitored. Users are informed how and why monitoring occurs; concerns identified are reported to the DSL.

16. Network Security

Technical security features (e.g., anti-virus, firewalls) are kept up to date by IT suppliers. Staff and students must not download unapproved software or open unfamiliar attachments and must report malware incidents.
All staff have unique usernames and private passwords. Passwords must be complex and are changed at least every 90 days. Lost credentials are handled by IT suppliers. Users must not share login details and must lock devices when not in use.

17. Emails

Email use is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality Policies. Approved Best Foot Forward email accounts are used for organisational work; personal accounts are not permitted during sessions.
Sensitive or personal information is sent only via secure, encrypted email. Spam/junk should be blocked and reported. Monitoring detects inappropriate links, malware and profanity. Chain letters and emails from unknown sources should be deleted without opening.
Phishing awareness includes:

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

Cyber-attacks via email are managed in line with the Cyber Response and Recovery Plan once complete.

18. Generative Artificial Intelligence (AI)

Best Foot Forward prepares students for emerging technologies, including generative AI, ensuring safe and age-appropriate use. Filtering and monitoring will limit access to harmful or inappropriate content and prevent the entry of personal/sensitive data into AI tools.

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

The CEO is responsible for overall website content and ensuring it is appropriate, accurate, up to date and compliant with government requirements.

21. Use of Devices

Staff and students may be issued Best Foot Forward-owned devices where necessary. Requirements for use are set out in the Device User Agreement.

22. Remote Learning

Remote learning is delivered in line with the Remote Education Policy, which sets out how online safety is considered when delivering remote education.

23. Monitoring and Review

Given the rapidly evolving online world, the DSL, IT suppliers and the CEO conduct half-termly light-touch reviews of this policy. The CEO and DSL review the policy annually and follow any online safety incidents. Changes are communicated to all members of the community.

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: Digital footprint, kindness online, cyberbullying responses; covered in PSHE and tutor time.
- Commerce: Advertising literacy, scams/phishing, in-app purchases; covered in Digital Skills.