Online Safety (Staff) Policy

Policy Code:	ICT2
Policy Start Date:	September 2025
Policy Review Date:	September 2026

Please read this policy in conjunction with the policies listed below:

- HR5 ICT Acceptable Use Policy
- HR6 Data Protection Policy
- HR6A Data Breach Policy
- HR12 Staff Disciplinary Policy
- HR22 Social Media (Staff) Policy
- HR23 Whistleblowing Policy
- HR24 Allegations of Abuse Made Against Adults Policy
- HR29 Code of Conduct
- HR41 Staff Anti-Bullying and Harassment Policy
- HR42 Low-Level Concerns Policy
- ICT3 Online Safety (Pupils) Policy
- SW4 Student Behaviour and Discipline Policy
- SW5 Safeguarding and Child Protection Policy
- SW6 Anti-Bullying Policy
- SW16 Freedom of Speech and Expression Policy
- SW17 Safeguarding Adults Policy

1 Policy Statement

1.1 The Priory Federation of Academies Trust (the Trust) takes online safety seriously. This policy is an extension of the ICT Acceptable Use Policy and is to provide a more detailed policy statement to ensure safe practice when working in the changing world of ICT.

1.2 References to the Trust or Academy within this policy specifically include all primary, secondary and special academies within the Trust, as well as the Early Years setting at the Priory Witham Academy, Priory Apprenticeships and Lincolnshire ITT.

1.3 This policy does not form part of any member of staff's contract of employment and it may be amended at any time.

2 Roles, Responsibilities and Implementation

2.1 The Pay, Performance and HR Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. This committee delegates day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Director of Central Services.

2.2 Leaders and Managers have a specific responsibility to ensure the fair application of this policy and all staff are responsible for supporting colleagues and ensuring its success.

2.3 This policy applies to all adults of the Trust community (including staff, volunteers, visitors, trainees, learners, trustees and governors) who have access to and are users of Trust ICT systems, both in and out of the settings. This policy should be read alongside ICT3 Online Safety (Pupils) Policy.

2.4 Headteachers/Heads of Setting have a duty of care for ensuring the safety (including online safety) of members of their community, although the day-to-day responsibility for online safety will be delegated to a nominated member of staff (as per Section 4).

2.5 The implementation of this policy will be monitored by a designated member of staff within each setting. This may be, but is not restricted to, the Designated Safeguarding Lead (DSL) or a member of the Senior Leadership Team (SLT). Each setting may, if they wish, appoint a designated Online Safety Coordinator who will then take responsibility for the implementation of this policy.

2.6 The Headteacher/Head of Setting and (at least) one other member of the Senior Leadership Team at each setting are to be aware of the procedures to be followed in the event of a serious online safety allegation being made against an adult (see Sections 22/23).

3 Aims

3.1 To ensure the Trust carries out its statutory responsibility to safeguard and promote the welfare of children in accordance with *Working Together to Safeguard Children*, *Keeping Children Safe in Education*, *the Prevent Duty Guidance* and the *Counter-Terrorism and Security Act 2015*.

3.2 To protect and safeguard the welfare of the children and young people entrusted to the Trust's care by establishing safe environments in which they can learn and develop.

3.3 To protect and safeguard the welfare of the Trust's staff by establishing safe working environments.

3.4 To ensure that all Trust members are empowered to use technology in a safe and responsible way.

4 The role of the Designated Member of Staff Responsible for Online Safety

4.1 The designated member of staff is responsible for:

- leading online safety at the setting;
- taking day-to-day responsibility for online safety issues and taking a leading role in establishing, implementing and reviewing the Trust's Online Safety Policy and supporting documents;
- undertaking suitable training to ensure they can carry out their role and train other colleagues, as relevant;
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- providing training and advice for staff;
- liaising with the Local Authority/other relevant body;
- liaising with Federation technical staff;
- working with the Designated Safeguarding Lead (DSL) to oversee and act on filtering and monitoring reports, as well as having an oversight of the checks carried out on the filtering and monitoring systems;
- generating reports of online safety incidents and using these to inform future online safety developments;
- meeting regularly with the setting's SLT to discuss current issues and review incident logs; and
- attending relevant meetings/committee meetings.

5 The role of the Designated Safeguarding Lead (DSL)

5.1 The DSL should be trained in online safety issues and be aware of the potential for serious safeguarding issues including:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate online contact with adults/strangers;
- potential or actual incidents of grooming, including sexual predation and sextortion;
- cyberbullying, including homophobic, biphobic and transphobic bullying;
- child-on-child abuse;
- extremism and radicalisation;
- child exploitation (criminal and sexual);
- sending nudes and semi-nudes;
- cybercrime;
- privacy and identity theft; and
- fake news and misinformation.

5.2 The DSL is also responsible for working with the Designated Member of Staff for Online Safety (if this is not the DSL) to oversee and act on filtering and monitoring reports, as well as having an oversight of the checks carried out on the filtering and monitoring systems.

6 The role of the Technical Support Team

6.1 The Technical Support Team is responsible for ensuring:

- that the Trust's technical infrastructure is secure and is not open to misuse or malicious attack;
- there are rules and configurations in place designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords will be encouraged to be over 8 characters long, made up of 3 words, with numbers or symbols;
- that the filtering policy is applied and updated on a regular basis;
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- that use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to senior leaders for investigation;

- that filtering and monitoring software/systems are implemented, maintained and updated as agreed in Trust policies, including identifying any risk and carrying out reviews and checks;
- documenting decisions on what is blocked or allowed (through the filtering system) and why; and
- community users are given limited access to the Trust network.

7 The role of Teaching and Support Staff

7.1 Teaching and Support Staff are responsible for ensuring that:

- they access and understand this policy, alongside HR29 Code of Conduct;
- they engage in training to ensure they have a good understanding of current online safety issues;
- they have read and understood HR5 ICT Acceptable Use Policy (AUP);
- when using social media, they adhere to HR22 Social Media (Staff) Policy;
- they have an up-to-date understanding of ICT3 Online Safety (Pupils) Policy and they take responsibility (where appropriate) for delivering the online safety curriculum to pupils;
- pupils understand and follow ICT3 Online Safety (Pupils) Policy and HR5 ICT Acceptable Use Policy;
- they report any suspected misuse or problem to senior staff for investigation/action/sanction;
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official Trust systems;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- they work with the Trust's technical team to ensure any community users for whom they have responsibility are given the appropriate level of access to the Trust network and they monitor the community user(s) to ensure that HR5 Acceptable Use Policy is adhered to; and
- they model good practice to children and young people with regards to safe and responsible use of technology.

8 Senior Leadership Team (SLT)

8.1 The setting's SLT, along with the Trust's management team, is responsible for:

- procuring filtering and monitoring systems; and
- overseeing any reports linked to filtering and monitoring.

9 The role of Parents/Carers

9.1 Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Each setting will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, pages on the Trust website and information about national/local online safety campaigns and literature. Parents/carers will be encouraged to support the settings in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Trust events (please see Section 16);
- access to parents/carers' sections of the website/Virtual Learning Environment and online pupil records; and
- their children's personal devices in the settings (where allowed).

10 Community Users

10.1 Community Users who access Trust systems/websites/Virtual Learning Environment as part of the wider Federation provision are expected to read HR5 ICT Acceptable Use Policy before they log in to any network resources. A reminder appears on screen for all new users for this and the policy is available externally on the Trust's website.

11 Governors

11.1 Each Academy's Local Governing Body (LGB) will have responsibility for reviewing the effectiveness of online safety within the setting.

The role of the LGB will be to:

- regularly monitor online safety incidents (through the Priory Profile). Governors must be prepared to challenge the information given to them if necessary and offer support where appropriate;
- regularly review the online safety provision within the setting; and
- appoint a governor, normally the Link Safeguarding Governor, who will have overall responsibility for filtering and monitoring.

12 Trustees

12.1 The Trust will review the overall effectiveness of this and ICT3 Online Safety (Pupils) Policy through regular reports from the Director of Safeguarding.

12.2 Trustees are responsible for ensuring that each setting has appointed an appropriate senior member of staff to the role of DSL, who will take lead responsibility for safeguarding, including online safety and understanding the filtering and monitoring systems and processes in place.

13 Education for Online Safety

13.1 Education - Pupils

Please see ICT3 Online Safety (Pupils) Policy.

13.2 Education - Parents/Carers

Each setting seeks to provide information and awareness to parents/carers through:

- curriculum activities;
- letters, newsletters, website, Virtual Learning Environment;
- information evenings/sessions for parents/carers;
- high-profile events and campaigns, e.g., Safer Internet Day; and
- reference to the relevant websites/publications.

13.3 Education – Staff/Volunteers

The Trust will seek to keep staff and volunteers' knowledge up-to-date by ensuring:

- online Safety is included within the Trust's safeguarding training, and staff are provided with safeguarding updates throughout the year;
- all new staff should receive training as part of their induction programme, ensuring that they fully understand the Trust's Online Safety policies and Acceptable Use Policy;
- the designated member of staff for Online Safety and the Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- this Online Safety Policy and its updates will be presented to, and discussed by, staff in staff meetings/training sessions;
- the Online Safety Coordinator (if applicable) will provide advice/guidance/training to individuals as required; and
- all teaching staff will make use of section 5 of ICT3 Online Safety (Pupils) Policy in their curriculum planning and teaching.

13.4 Education – Governors and Trustees

Governors and Trustees should take part in online safety training/awareness sessions, with particular importance for the governor whose role incorporates child protection. This may be offered in a number of ways:

- attendance at training provided by the Local Authority/National Governors Association or other relevant organisation;
- participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons);
- online training through an accredited provider; and/or
- participation in training sessions held at the Local Governing Body Meeting.

14 Technical Strategy

14.1 There will be regular discussions and audits of the safety and security of Trust technical systems through the weekly IT management meetings.

14.2 Servers, wireless systems and cabling are securely located and physical access restricted.

14.3 All users have clearly defined access rights to the setting's technical systems and devices.

14.4 The Trust uses an intelligent system to monitor internet usage which responds to patterns of behaviour and intelligently scans pages for inappropriate content.

14.5 Federation technical staff regularly monitor and record the activity of users on the Trust's technical systems and users are made aware of this in HR5 ICT Acceptable Use Policy.

14.6 An agreed procedure is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the Trust systems.

14.7 Staff and pupils are restricted from downloading executable files and installing programmes on Trust devices.

15 Filtering and monitoring

15.1 In respect of filtering and monitoring, the Trust will adhere to the DfE document *Meeting digital and technology standards in schools and colleges.*

15.2 The Trust uses a filtering system (Smoothwall) for its wired devices and for its wireless devices.

15.3 Each setting will have an assigned member of the senior leadership team, normally the Designated Safeguarding Lead, and a governor, normally the Link Safeguarding Governor, who will have overall responsibility for filtering and monitoring.

15.4 The Trust's filtering and monitoring provision will be reviewed on an annual basis, or sooner if required.

15.5 The Trust monitors user activity in the following ways:

- Designated Safeguarding Leads are notified each day of any instances where users have been blocked by the filtering system (through network monitoring). The DSL can then follow this up in accordance with the setting's safeguarding procedures. This is also accessible to the Trust DSL, for monitoring where necessary;
- physical monitoring of student use by staff in lessons, extra-curricular and lunchtime clubs and homework clubs;
- through the use of an intelligent system to monitor internet usage, which responds to patterns of behaviour and intelligently scans pages for inappropriate content;
- Trust technical staff regularly monitor and record the activity of users on the Trust's technical systems and users are made aware of this in HR5 ICT Acceptable Use Policy; and
- internet reporting databases are maintained at each site so that a history can be built up for investigations into individuals if required.

15.6 Internet access is filtered for all users. Illegal content (e.g., child sexual abuse images) is filtered by the filtering provider. The Trust will also establish appropriate levels of filtering to ensure pupils are safe from terrorist and extremist material. Content lists are regularly updated and internet use is logged and regularly monitored.

15.7 Whilst internet access is filtered for all users, pupils will not be subject to 'over blocking' and instead will be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

15.8 Staff and pupils can request for filters to be taken off specific sites, where technical staff will assess suitability and escalate to senior staff if needed.

15.9 The Trust has enhanced/differentiated user-level filtering with different restrictions for user groups, e.g., staff, pupils, etc.

15.10 Monitoring systems are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the Trust's

systems and data. These are tested regularly (both internally and externally). The Trust's infrastructure and individual workstations are protected by up-to-date anti-virus software.

16 Bring Your Own Device (BYOD)

16.1 Staff are allowed to bring their own devices into certain areas of the Trust (please refer to SW5 Child Protection and Safeguarding Policy). When bringing their own device, staff should adhere to the following:

- they should use the secure virtual desktop or Microsoft 365 systems for application access;
- if required, the device should be connected to the Trust's filtered wireless; if an individual chooses to use their own mobile data (e.g., 3G/4G/5G) on the site then they should ensure they comply with HR5 ICT Acceptable Use Policy at all times;
- staff must not use their own personal devices to take photographs or videos or record events (audio/video) of pupils and/or Trust activities; and
- staff must not store personal data or sensitive personal data relating to the Trust on their own personal devices.

17 Use of digital and video images

17.1 When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the internet, e.g., on social networking sites.

17.2 In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Trust events for their own personal use (as such use is not covered by the Data Protection Act 2018) providing they have sought permission from the relevant setting. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

17.3 Staff and volunteers are allowed to take digital/video images to support educational aims, however, these images should only be taken on Trust equipment; the personal equipment of staff should not be used for such purposes. Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities which might bring the individuals or the Trust into disrepute.
Staff must only take images/videos where explicit consent has been given.

17.4 Pupils must not take, use, share, publish or distribute images of others without their permission.

17.5 Photographs published on the website or elsewhere that include pupils will be selected carefully to protect the identity of the pupil and to ensure the Trust's commitment to safeguarding children and young people is upheld.

17.6 A pupil's full name will not be associated with a photograph. Only in exceptional circumstances, e.g., the success of a known Head Girl/Boy, will this be considered and permission will always be gained from the pupil and their parents/carers before it is published.

17.7 Permission from parents/carers to use pupils' pictures and videos in Trust work and promotion is taken when pupils join the relevant setting. When pupils turn 14, this permission is collected again, but from the pupil themselves (where appropriate).

18 Unsuitable/inappropriate activities

18.1 The Trust requires staff not to engage in unsuitable or inappropriate activities in school or outside school when using Trust equipment or systems as they risk both the safety of staff and reputation of the Trust. Such activities, in addition to unlawful behaviour, might include accessing pornography, promoting discrimination, threatening behaviour, racist material and any other actions which breach the principles of this policy.

18.2 Social Media - Protecting Professional Identity

Please see HR22 Social Media (Staff) Policy.

18.3 User Actions

Some internet activity (e.g., accessing child abuse images or distributing racist material) is illegal and is banned from Trust and all other technical systems and could lead to criminal prosecution. Other inappropriate activities (e.g., cyber bullying) are also banned.

The Trust believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using the Trust's equipment or systems. Some examples of restricted usage can be seen over the page.

		Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**		X
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003.		X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008		X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986		X
	Articles, images, speeches or videos that promote terrorism; content encouraging people to commit acts of terrorism; websites made by terrorist organisations; videos of terrorist attacks.		X
	Sending or delivering letters or other articles for the purpose of causing distress or anxiety (this includes electronic communication). Contrary to the Malicious Communications Act 1988.		X
	Pornography	X	
	Promotion of any kind of discrimination	X	
	Threatening behaviour, including promotion of physical violence or mental harm	X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	X	
Using school systems to run a private business		X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust		X	
Infringing copyright		X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)		X	
Creating or propagating computer viruses or other harmful files		X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)		X	

19 Reporting incidents of misuse

19.1 The Trust has a duty of care to all pupils and staff to ensure they are safe to work, learn and develop unimpeded by fear.

19.2 Any incidents of misuse must be reported to a member of the SLT or the DSL as soon as possible. Any reported incidents will be taken seriously. If staff have concerns about an adult, this must be reported in line with the Trust's safeguarding procedures. Please refer to HR24 Allegations of Abuse Made Against Adults and HR42 Low-Level Concerns Policy.

19.3 Where bullying is found to have taken place by any means, whether on-site or off-site, including cyber bullying, robust action will be taken to protect the well-being of pupils and staff.

19.4 In all our communications, whether written, spoken, texted, emailed or published on websites, we must treat other people with respect. Even if we disagree with another person, fall out with them, or become angry with them, we should state our case clearly and respectfully.

19.5 Staff can, if they wish, refer to HR23 Whistleblowing Policy.

20 Responding to incidents of misuse involving pupils

20.1 If there is any suspicion that any pupil has been involved in inappropriate or unsuitable activity the DSL or a Designated Safeguarding Officer (DSO) at the relevant setting is to be contacted immediately.

The contact details for the DSL and DSOs of each setting will be posted appropriately throughout the setting and all staff are to be made aware of the DSL and DSOs at staff briefings on a regular basis and as part of staff induction. In the event that a DSL or a DSO is not immediately available, a member of the Senior Leadership Team is to be alerted at once (in line with the Trust's safeguarding procedures).

20.2 The DSL/DSO/Senior Leader will notify the Headteacher and an appropriate member of staff will be identified to investigate any reports and to determine what, if anything, has occurred. If appropriate, the Trust DSL will also be informed. The Trust DSL is available outside work hours on 01522 871355. The setting DSL or Trust DSL will notify the police if necessary.

20.3 Incidents of misuse involving pupils will be dealt with in accordance with the Trust's SW4 Student Behaviour and Discipline Policy.

21 Safeguarding incidents involving an adult working with the Trust's children and young people

21.1 If there is any suspicion that the online activity (e.g., website(s) visited) of a member of staff constitutes a safeguarding concern then staff must report this as outlined in HR24 Allegations of Abuse Made Against Adults Policy. If staff feel that their concern is a low-level concern about an adult working with the Trust's children, they should adhere to the referral processes outlined in HR42 Low-Level Concerns Policy.

22 Other incidents involving an adult working with the Trust's children and young people

22.1 It is expected that all members of the Trust community will be responsible users of digital technologies, and will understand and follow Trust policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, deliberate misuse.

23 Investigating incidents of misuse

23.1 In the event of alleged or known misuse, all steps in this procedure should be followed:

- if there is any suspicion that a member of staff (including volunteers, visitors, supply staff, contractors, governors or Trustees) has been involved in inappropriate or unsuitable activity, the Headteacher/Head of Setting is to be contacted immediately. In the event that the Headteacher/Head of Setting is not immediately available, the Trust DSL should be informed;
- the Headteacher will inform the Trust DSL and the Head of HR, who will manage the concern in line with the Trust's HR12 Staff Disciplinary Policy, HR24 Allegations of Abuse Made Against Adults Policy and HR42 Low Level Concerns Policy (as appropriate);
- the investigation should be conducted in collaboration with a member of the systems team who will be able to provide any relevant data to the investigation;
- it is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection); and
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and retained in an evidence file (except in the case of child abuse images – see 23.3).

23.2 Once the investigation has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- internal response or continuing disciplinary procedures;
- referral to Local Authority Designated Officer (LADO);
- Police involvement and/or action; and/or
- involvement by Local Authority or national/local organisation (as appropriate).

23.3 If content being reviewed includes images of child abuse, then the monitoring/investigation should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour;
- the sending of obscene materials to a child;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material; and/or
- other criminal conduct, activity or materials.

23.4 The user's account will have suspended access until the investigation is complete.

23.5 It is important that all of the above steps are taken as they will provide an evidence trail for the Trust and possibly the Police, and demonstrate that visits to any sites were carried out for child protection purposes. The file should be retained by the group for evidence and reference purposes.

24 Development, Monitoring and Review

24.1 This policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

24.2 The settings will monitor the impact of the policy using: logs of reported incidents through the pastoral systems; monitoring logs of internet activity (including sites visited); internal monitoring data for network activity; surveys/questionnaires of pupils, parents/carers and staff.

25 Policy change

25.1 This policy may only be amended or withdrawn by the Priory Federation of Academies Trust.

The Priory Federation of Academies Trust
Online Safety (Staff) Policy

This Policy has been approved by the Trust's Pay, Performance and HR Committee.

Signed…… Name..... Date:

Trustee

Signed…… Name..... Date:

Chief Executive Officer

Signed…… Name..... Date:

Designated Member of Staff

Please note that a signed copy of this agreement is available via Human Resources.