Online Safety (Pupils) Policy

Policy Code:	ICT3
Policy Start Date:	September 2023
Policy Review Date:	September 2024

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

- HR5 ICT Acceptable Use Policy
- HR6 Data Protection Policy
- HR6A Data Breach Policy
- ICT2 Online Safety (Staff) Policy
- SW4 Pupil 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 HR5 ICT Acceptable Use Policy and SW5 Safeguarding and Child Protection Policy and is to provide a more detailed policy statement to ensure safe practice when working in the changing world of ICT.

1.2 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other online safety incidents covered by this policy, which may take place outside of the setting, but are linked to membership of the academy/setting or Trust and/or may bring the reputation of the academy/setting or Trust into disrepute.

1.3 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 SCITT.

1.4 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 Strategic IT Coordinator.

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

2.3 This Policy applies to all children, young people and vulnerable adults whose care and education comes within the remit of The Trust. This policy should be read alongside ICT2 Online Safety (Staff) Policy, which applies to all adult members of The Trust community.

2.4 The Headteacher/Head of Setting has a duty of care for ensuring the safety (including online safety) of members of the setting community, although the day-to-day responsibility for online safety will be delegated to a nominated member of staff (as per Section 4 of ICT2 Online Safety (Staff) Policy).

2.5 The implementation of this Online Safety 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.

3 Aims

3.1 To ensure that the Trust carries out its statutory responsibility to safeguard and promote the welfare of children in accordance with *Working Together to Safeguard Children 2018*, *Keeping Children Safe in Education 2023*, the *Prevent Duty Guidance 2015* 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 ensure that all Trust members are empowered to use technology in a safe and responsible way.

4 Pupils

4.1 Pupils are responsible for using the Trust's digital technology systems in accordance with the Trust's HR5 ICT Acceptable Use Policy and this Online Safety Policy. This information is signposted to pupils at the beginning of each academic year by the pastoral teams, and each time they log in.

5 Education about Online Safety

5.1 A planned online safety curriculum will be provided as part of Computing and Personal Development lessons. This is reviewed annually (or sooner if an issue occurs which requires attention). The purpose of the online safety curriculum is to empower young people to be safe and responsible users of technology.

5.2 The breadth of issues classified within online safety is considerable, thus the topics covered within the curriculum will change over time to reflect the changing use of technology. However, each setting's curriculum will be built around four identified areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material;
- Contact – being subjected to harmful online interaction with other users;
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm; and

- Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

5.3 Content is likely to be broken down into the following areas:

- Self-image and identity.
- Online relationships.
- Online reputation.
- Online bullying.
- Managing online information.
- Health, wellbeing and lifestyle.
- Privacy and security.
- Copyright and ownership.

5.4 The Online safety curriculum will include, but is not restricted to, the following topics: Child Exploitation; Radicalisation and Extremism; Sexual Predation; Cyber bullying, including homophobic, biphobic and transphobic bullying; Child-on-Child Abuse.

6 User access

6.1 All users have clearly defined access rights to Trust technical systems and devices.

6.2 All users (in some primary contexts, a shared log-in is used initially) will be provided with a username and secure password. Users are responsible for the security of their username and password.

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

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

7 Filtering and monitoring

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

7.2 The Trust uses a filtering system (Smoothwall) for its wired devices, and a further filtering system (Fortinet) for its wireless devices.

7.3 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.

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

7.5 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.
- Internet reporting databases are maintained at each site so that a history can be built up for investigations into individuals if required.

7.6 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.

7.7 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.

7.8 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.

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

7.10 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.

8 Bring Your Own Device (BYOD)

8.1 Staff and pupils are allowed to bring their own devices into certain lessons and areas of the Trust.

- Users are encouraged to use the secure virtual desktop or Microsoft 365 systems for application access.
- Filtered wireless internet is available to users in the Trust.
- The Academies have a set of clear expectations and responsibilities for all users.
- The Trust adheres to the Data Protection Act (2018) principles.
- All network systems are secure and access for users is differentiated.
- All users will use their username and password and keep this safe.
- Regular audits and monitoring of usage will take place to ensure compliance.
- If pupils wish to use internet services on their own device the Trust-provided wifi services are recommended as these are monitored and managed; however, if an individual chooses to use their own mobile data (e.g. 3G/4G/5G) on a Trust site then they should ensure they comply with the Acceptable Use Policy at all times.
- Pupils must not store personal data or sensitive personal data relating to the Trust on their own personal devices.
- Whilst on any Trust site pupils must not record events (audio/video) or take photographs on any personal device (including mobile phones), unless given permission by a member of staff.

8.2 Digital Devices

- Pupils are permitted to bring their own digital devices onto site, providing they meet Trust expectations (as outlined above) with regard to the use of such devices.
- Pupils must ensure at all times that any use of their digital devices on a Trust site is in line with this policy and HR5 ICT Acceptable Use Policy. This applies to pupils using their devices on a Trust site even if their device is not connected to the Trust network and they are using their own personal data (e.g. 3G/4G/5G).

9 Use of digital and video images

9.1 When using digital images, pupils will be informed and educated 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.

9.2 Pupils must seek permission from the relevant setting if they wish to take videos and digital images of other pupils at Trust events for their own personal use (as such use is not covered by the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social

networking sites unless they have the explicit consent of the individuals in the video or image.

9.3 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.

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

9.5 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 school's commitment to safeguarding children and young people is upheld.

9.6 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.

9.7 Permission from parents/carers to use pupils' pictures and videos in school work and promotion is taken when pupils join the school.

10 Unsuitable/inappropriate activities

10.1 Pupils should not engage in unsuitable or inappropriate activities in school or outside school when using Trust equipment or systems as they risk both the pupil's safety and the reputation of the Trust and its academies. Unsuitable or inappropriate activities, in addition to unlawful behaviour, include accessing pornography, promoting discrimination, threatening behaviour, racist material and any other actions which breach the principles of this Online Safety Policy.

10.2 The setting will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of the setting.

10.3 Cyber-bullying

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 wellbeing of pupils and staff (please refer to SW6 Anti-Bullying Policy).

Advice given to pupils
Guidance and advice will be provided to pupils through each setting's Personal Development (PD) programme. The text below forms the basis of how this advice is communicated directly to young people.

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. Others should always be treated with tolerance and respect.

- *If you feel you are being bullied by email, text or online, do talk to someone you trust, if possible an adult*
- *Never send any bullying or threatening messages. Anything you write and send could be read by an adult. Stop and think before you send.*
- *Bullying should be reported to a member of staff or trusted adult; in some cases the setting will inform the police - for example, threats of a sexual nature.*
- *Keep and save any bullying emails, text messages or images.*
- *If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.*
- ***Don't** reply to bullying or threatening text messages or emails - this could make matters worse. It also lets the offenders know that they have found a 'live' phone number or email address. They may get bored quite quickly if you ignore them.*
- ***Don't** forward abusive texts or emails or images to anyone. You could be breaking the law just by forwarding them. Do not reply to the sender.*
- ***Don't** ever give out passwords to any of your accounts.*
- ***Remember** that sending abusive or threatening messages is against the law.*

10.4 Sharing nudes and semi-nudes

The sharing of nudes and semi-nudes, previously known as 'sexting' is the exchange of sexually explicit images, through mobile picture messages or webcams over the internet. These images are often, but not always, self-generated.

Under British law it is illegal and a serious criminal offence to take, hold or share "indecent" photos of anyone aged under 18, even if the image has been produced and/or sent with the consent of the individual in the image. As such, the Trust will not condone any behaviour of this kind.

As part of the curriculum, pupils will be educated and informed about the risks associated with such behaviour. There will also be a focus on improving self-esteem and promoting positive relationships. Sharing nudes and semi-nudes is one way in which child-on-child abuse can manifest itself and so it is essential that pupils understand and actively work towards promoting respectful and positive relationships. For further information, see SW5 Safeguarding and Child Protection Policy.

10.5 Examples of Inappropriate User Actions

The Trust believes that the activities referred to in the following section would be inappropriate in an Academy context and that pupils should not engage in these activities in or outside of the setting when using Trust equipment or systems. Some examples of restricted usage are as follows:

		Acceptable at certain times	Acceptable for nominated users	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 Academy or brings the Academy into disrepute			X	
Using Trust 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	
File sharing		X			
Use of social media		X			
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube		X			

11 Reporting incidents of misuse

11.1 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. Pupils are encouraged to report any incidents of misuse to a member of staff or trusted adult immediately. Any reported incidents will be taken seriously.

11.2 If a pupil has concerns or suspicions that a member of staff may be involved in an incident of misuse, which would normally include communicating or making a connection with a pupil via social media, they should report this to the Headteacher/Head of Setting immediately.

11.3 Incidents involving pupils

- 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, in line with Trust safeguarding procedures.

- The contact details for the DSL and DSOs of each setting will be posted appropriately throughout the setting (and on the website) 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. Pupils should also be made aware of who the DSL and DSO are. In the event that a DSL or 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).

- The DSL/DSO/Senior Leader will notify the Headteacher/Head of Setting 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 during and outside working hours on 01522 871355. The DSL or Trust DSL will notify the police if necessary.

- If appropriate, the Trust DSL or the Head of HR will notify the Local Authority Designated Officer (LADO).

- If a pupil has a suspicion that any Trust user may be accessing a website which contains child abuse images, or if there is any other suspected illegal activity, they must inform a member of staff (or trusted adult) immediately.

- Incidents of misuse involving pupils will be dealt with in accordance with SW4 Pupil Behaviour and Discipline Policy.

12 Development, Monitoring and Review

12.1 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.

12.2 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.

13 Policy change

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

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

This Policy has been approved by the 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.