E-Safety Policy

Policy Code:	ICT2
Policy Start Date:	September 2017
Policy Review Date:	September 2018

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

- HR5 ICT Acceptable Use Policy
- HR23 Whistleblowing Policy
- ICT3 E-Safety Policy (Students)
- SW4 Student Behaviour and Discipline Policy
- SW5 Safeguarding and Child Protection Policy
- SW6 Anti-Bullying Policy
- SW16 Freedom of Speech and Expression Policy
- Staff Disciplinary Policy

1. Policy Statement

- The Priory Federation of Academies Trust (The Trust) takes e-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.
- This policy applies to all members of The Trust community (including staff, students, volunteers, parents/carers, visitors, trustees, governors) who have access to and are users of Trust ICT systems, both in and out of the Academy. This policy should be read alongside ICT3 E-Safety Policy (Students).
- The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 e-safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy or Trust and/or may bring the reputation of the Academy or Trust into disrepute.
- The Academy will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the Academy.

2. Policy Details

2.1 Introduction

- This policy sets out how The Trust is carrying out its statutory responsibility to safeguard and promote the welfare of children in accordance with *Working Together to Safeguard Children 2015*, *Keeping Children Safe in Education 2016*, *the Prevent Duty Guidance 2015* and the *Counter-Terrorism and Security Act 2015*. The Trust will also follow the guidance contained in *Meeting the Needs of Children in Lincolnshire 2014*.
- Where Academies are mentioned throughout, this also includes the Robert de Cheney Boarding House at The Priory Academy LSST, The Keyworth Centre at The Priory City of Lincoln Academy and the Early Years setting at The Priory Witham Academy, as well as the Trust's French Centre.

2.2 Principles

- The Trust recognises its responsibility to protect and safeguard the welfare of the children and young people entrusted to its care by establishing safe environments in which they can learn and develop.

- The Trust recognises its responsibility to protect and safeguard the welfare of its staff by establishing safe working environments.
- The use of technology has become a significant component of many safeguarding issues, thus The Trust recognises the need for an effective approach to online safety.
- The Trust will ensure that all its members are empowered to use technology in a safe and responsible way. This will be managed through training, clear reporting procedures and risk assessment.
- The Trust promotes a positive, supportive and secure ethos, giving all its members a sense of being valued.

3. Responsibilities

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the Academy community, although the day-to-day responsibility for e-safety will be delegated to a nominated member of staff (as per Section 3.1).
- The implementation of this E-Safety Policy will be monitored by a designated member of staff within each Academy. This may be, but is not restricted to, the Designated Safeguarding Lead (DSL) or a member of the Senior Leadership Team (SLT). Each Academy may, if they wish, appoint a designated E-Safety Coordinator who will then take responsibility for the implementation of this policy.
- The Headteacher and (at least) one other member of the Senior Leadership Team at each Academy are to be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see Section 9).

3.1 Designated Member of Staff Responsible for E-safety

The designated member of staff is responsible for:

- Leading e-safety at the Academy.
- Taking day-to-day responsibility for e-safety issues and taking a leading role in establishing, implementing and reviewing the Trust's E-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 e-safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority/other relevant body.
- Liaising with Federation technical staff.
- Generating reports of e-safety incidents and using these to inform future e-safety developments.

- Meeting regularly with the Academy's SLT and the Director of Student Welfare to discuss current issues and review incident logs.
- Attending relevant meetings/committee meetings.

3.2 The Designated Safeguarding Lead (DSL)

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

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming, including sexual predation.
- Cyber bullying, including homophobic, biphobic and transphobic bullying.
- Peer-on-peer abuse.
- Extremism and radicalisation.
- Child sexual exploitation.

3.3 Technical Support Team

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.
- That each Academy meets required e-safety technical requirements and any E-Safety Policy requirements that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords will be encouraged to be complex and changed regularly.
- That the filtering policy is applied and updated on a regular basis.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-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 monitoring software/systems are implemented and updated as agreed in Trust policies.
- Community users are given limited access to the Trust network.

3.4 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current Trust E-Safety Policy.
- They have an up-to-date understanding of the E-Safety Policy (Students) and they take responsibility for delivering the e-safety curriculum to students.
- They have read and understood HR5 ICT Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to senior staff for investigation/action/sanction.
- All digital communications with students/parents/carers should be on a professional level and only carried out using official Academy systems.
- Students understand and follow ICT3 E-Safety (Students) Policy and HR5 ICT Acceptable Use Policy.
- Students 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 Academy activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, students 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.
- When using social media they adhere to HR22 Social Media (Employee) Policy.
- They work with the Academy'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 the Acceptable Use Policy is adhered to.

3.5 Students

Students are responsible for:

- Using the Trust digital technology systems in accordance with the Trust's HR5 ICT Acceptable Use Policy and the ICT3 E-Safety Policy (Students).

3.6 Parents/Carers

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 Academy will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, pages on the Academy website and information about national/local e-

safety campaigns and literature. Parents/carers will be encouraged to support the Academies in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at Academy events (please see Section 7).
- Access to parents' sections of the website/Virtual Learning Environment and online student records.
- Their children's personal devices in the Academies (where this is allowed).

3.7 Community Users

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

3.9 Governors

In each Academy there will be a nominated member of the local governing body who will take on responsibility for reviewing the effectiveness of this policy. This is likely to be the governor who has responsibility for child protection.

The role of the E-Safety governor will be to:

- Attend meetings with the designated member of staff responsible for e-safety (at least one per year).
- Regularly monitor the e-safety incidents log. The governor must be prepared to challenge the information given to them if necessary and offer support where appropriate.
- Report any e-safety issues to the Committee at the Academy Committee meetings.

3.10 Trustees

The Trust will review the overall effectiveness of this and ICT3 E-Safety Policy (Students) through regular reports from the Director of Student Welfare.

4. Education for E-Safety

4.1 Education - Students

This is dealt with in a separate policy for students. Please see ICT3 E-Safety (Students).

4.2 Education - Parents/Carers

Each Academy 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.
- Reference to the relevant websites/publications. A series is published on each Academy's website.

4.3 Education – Staff/Volunteers

- A planned programme of formal e-safety training will be made available to staff. This is reviewed annually (or sooner if an issue occurs which requires attention).
- All new staff should receive training as part of their induction programme, ensuring that they fully understand the Trust's E-Safety Policies and Acceptable Use Policy.
- The designated member of staff for e-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 E-Safety Policy and its updates will be presented to, and discussed by, staff in staff meetings/training sessions.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.
- All teaching staff will make use of section 4 of ICT3 E-Safety (Students) Policy in their curriculum planning and teaching

4.4 Education – Governors and Trustees

Governors and trustees should take part in e-safety training/awareness sessions, with particular importance for the governor whose role incorporates e-safety and 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.

5. Technical Strategy

- There will be regular discussions and audits of the safety and security of Academy technical systems through the weekly IT management meetings.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to Academy technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password.
- Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider. The Trust will also establish appropriate levels of filtering to ensure students are safe from terrorist and extremist material. Content lists are regularly updated and internet use is logged and monitored.
- The Trust uses an intelligent system to monitor internet usage which responds to patterns of behaviour and intelligently scans pages for inappropriate content.
- Staff and students can request for filters to be taken off specific sites, where technical staff will assess suitability and escalate to senior staff if needed.
- The Trust has enhanced/differentiated user-level filtering with different restrictions for user groups, e.g. staff, boarders etc.
- 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.
- 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. The Trust infrastructure and individual workstations are protected by up-to-date anti-virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the Academy systems.
- Staff and students are restricted from downloading executable files and installing programmes on school devices.

6. Bring Your Own Device (BYOD)

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

- Users are encouraged to use the secure virtualisation systems for application access.
- Filtered wireless internet is available to users in the Trust.
- In boarding, a monitored, but more relaxed filtering system is used.
- The Academies have a set of clear expectations and responsibilities for all users, set out in HR5 ICT Acceptable Use Policy.
- The Trust adheres to the Data Protection Act 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 users wish to use internet services on their own device the Trust-provided wi-fi services are recommended as these are monitored and managed; however, if an individual chooses to use their own mobile data (e.g. 3G/4G) on the Academy 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 of students and/or Academy activities.

7. Use of digital and video images

- When using digital images, staff inform and educate students 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use is not covered by the Data Protection Act) providing they have sought permission from the relevant Academy. 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 students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, however, these images should only be taken on Academy equipment; the personal equipment of staff should not be used for such purposes. Staff must follow Trust policies concerning the sharing, distribution and publication of those images (see HR22 Social Media (Employee) Policy). Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities which might bring the individuals or the Academy into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website or elsewhere that include students will be selected carefully to protect the identity of the student and to ensure the school's commitment to safeguarding children and young people is upheld.
- A student'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 student's parents/carers before it is published.
- Permission from parents/carers to use students' pictures and videos in Academy work and promotion is taken when students join the Academy.

8. Unsuitable/inappropriate activities

The Trust requires staff not to engage in unsuitable or inappropriate activities in school or outside school when using Academy equipment or systems as they risk both the safety of staff and reputation of the Trust and its academies. 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 E-Safety Policy.

8.1 Social Media - Protecting Professional Identity

The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the Trust:

- Training, including acceptable use, social media risks, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

Academy staff should ensure that:

- No reference is to be made in social media to students, parents/carers or Academy staff and that they do not engage in online discussion on personal matters relating to members of the Academy and/or the Trust community.
- Personal opinions are not to be attributed to the Trust, the Academy or the local governing body.
- They regularly check security settings on personal social media profiles to minimise risk of loss of personal information.

- They have read and are aware of HR22 Social Media (Employee) Policy which is available on the Trust's website.

8.2 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 be 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 are as follows:

		Acceptable	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 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 school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg 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 eg Youtube		X				

8.3 Reporting incidents of misuse

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

Staff and students are encouraged to report any incidents of misuse to a member of staff (or other trusted adult) immediately. Any reported incidents will be taken seriously by The Trust.

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 students and staff.

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.

Staff wishing to report concerns about other members of staff may wish, if they feel it is appropriate, to refer to HR23 Whistleblowing Policy (found on the Trust's website).

9. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

9.1 Incidents involving students

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

The contact details for the DSL and DSOs of each Academy will be posted appropriately throughout the Academy 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).

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 DSW will also be informed. The DSW is available outside Academy hours on 4355 (internally) or 01522 871355. The DSW or DSL will notify the police if necessary.

If appropriate either the Academy DSL, the DSW or the Head of HR will notify the Local Authority Designated Officer (LADO) accordingly.

If a student has a suspicion that any Academy 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 students will be dealt with in accordance with the Trust's SW4 Student Behaviour and Discipline Policy.

9.2 Safeguarding incidents involving a member of staff

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 should follow the referral process in line with *Keeping Children Safe in Education 2016*.

If staff members have safeguarding concerns about another staff member then this should be referred to the Headteacher. Staff, however, if they wish can discuss any concerns with, and make a referral to, the Academy's DSL, who will then inform the Headteacher. If the concern involves the Headteacher, it must be passed to the DSL who will inform the Chief Executive. Any allegations should be immediately discussed with the Designated Officer (DO – previously LADO).
If the concern involves a member of the Trust's central staff, this should be referred to the Academy DSL who will inform the Chief Executive. If the concern involves the Chief Executive, this should be referred to the Academy DSL who must inform the Chair of The Trust immediately and advice should be sought from the DO (see HR24 Allegations of Abuse Against Staff Policy).

9.3 Other incidents involving a member of staff

It is hoped 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.

In the event of suspicion, all steps in this procedure should be followed:

- If there is any suspicion that member of staff (including volunteers, visitors and governors) has been involved in inappropriate or unsuitable activity, the DSL at the relevant Academy is to be contacted immediately. 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 and the Director of Student Welfare (DSW). The DSW will notify the police if necessary.
- If appropriate, either the Academy DSL, the DSW or the Head of HR will notify the Designated Officer (DO) accordingly.
- If the incident involves a member of staff the DSW and/or Head of HR will decide the nature of any investigation, in line with the Trust's Staff Disciplinary Policy.
- More than one senior member of staff/volunteer should be involved in any investigation process. This is vital to protect individuals if accusations are subsequently reported.
- 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).
- 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 below).

Once this 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.
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring 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.
- Other criminal conduct, activity or materials.

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

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 these sites were carried out for child protection purposes. The file should be retained by the group for evidence and reference purposes.

10. Development, Monitoring and Review

- 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 e-safety or incidents that have taken place.

- The DSL in each Academy will produce a report for their local governing body at least once a year on the implementation of the E-Safety Policy (which will include anonymous details of any e-safety incidents).
- The Academies 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 students, parents/carers and staff.

11. Policy change

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

The Priory Federation of Academies Trust
E-Safety Policy

This Policy has been approved by the Trust's Education and Standards 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.