The Priory Federation Of Academies Trust

E-Safety Policy

Policy Code:	ICT2
Policy Start Date:	July 2015
Policy Review Date:	September 2015

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

- SW5 Safeguarding and Child Protection Policy
- HR5 ICT Acceptable Use Policy
- HR22 Social Media (Employee) Policy
- Staff Disciplinary Policy
- HR23 Whistleblowing Policy
- SW6 Anti-Bullying Policy

1. Policy Statement

The Priory Federation of Academies Trust, hereafter known as 'The Trust', takes e-safety seriously. This policy is an extension of the ICT Acceptable Use Policy and is to provide guidance and procedures 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, governors) who have access to and are users of Federation ICT systems, both in and out of the Academy.

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 Federation.

The Academy will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the Academy.

2. Schedule for Development, Monitoring and Review

The implementation of this E-Safety policy will be monitored by the:	E-safety Coordinator; Designated Safeguarding Officer; Director of Student Welfare; The Trust.
Monitoring will take place at regular intervals:	Annually.
The Academy Committee members will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	At each Academy Committee meeting (3 times a year).
The E-Safety 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 next anticipated review date will be:	September 2015.
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Academy Designated Safeguarding Officer; LADO (Local Authority Designated Officer); Director of Student Welfare; Police; Academy SLT.

2.1 Review

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.

3. Responsibilities

This E-Safety Policy has been developed by a working group of the Executive Committee, Strategic IT Coordinator, Staff (including teachers, support staff and technical staff) and Governors.

3.1 General

- 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, to be known as the E-Safety Co-ordinator.
- 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).
- The Senior Leadership Team will receive monitoring reports from the E-Safety Co-ordinator.

3.2 E-Safety Co-ordinator

The E-Safety Co-ordinator is responsible for:

- Leading e-safety at the Academy.
- Taking day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the Trust's E-Safety Policy/supporting documents.
- Undertaking suitable training to ensure they can carry out their role and to 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/relevant body.
- Liaising with Federation technical staff.
- Receiving reports of e-safety incidents and using these to inform future e-safety developments.
- Meeting regularly with the Director of Student Welfare to discuss current issues, review incident logs and control logs

- Attending relevant meetings/committee meetings.
- Reporting regularly to Senior Leadership Team.

3.3 The Designated Safeguarding Officer

The DSO should be trained in e-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

3.4 Technical Support Team

The Technical Support Team is responsible for ensuring:

- That the Academies' 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 guidance 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.

3.5 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 read and understood the Staff Acceptable Use Policy (AUP) and signed the agreement.

- 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 the E-Safety and Acceptable Use Policies.
- 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 the Social Media (Employee) Policy.

3.6 Students

Students are responsible for:

- Using the Federation digital technology systems in accordance with the Acceptable Use Policy.

They will also:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Be expected to know, understand and adhere to this policy with regards to the use of mobile devices and digital cameras and the taking/use of images and on cyber-bullying.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Trust's E-Safety Policy covers their actions out of school, if related to their membership of the school.

3.7 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 understand these issues through parents' evenings, newsletters, letters, pages on the Academy website and information about national/local e-safety campaigns and literature. Parents and 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.
- 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).

3.8 Community Users

Community Users who access Academy systems/websites/Virtual Learning Environment as part of the wider Federation provision will be expected to read the 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 Federation website.

3.9 Governors

In each Academy there will be a nominated member of the Committee 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 regular meetings with the E-Safety Co-ordinator.
- Regularly monitor the e-safety incidents log.
- Report any e-safety issues to the Committee at the Academy Committee meetings.

4 Education of E-Safety

4.1 Education - Students

E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.

- A planned e-safety curriculum is provided as part of Computing and PDP lessons. This is reviewed annually (or sooner if an issue occurs which requires attention).
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Key messages on self-esteem and positive relationships are reinforced through the PDP curriculum.
- Students are taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

- Students are helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the Academy.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- Where students are allowed freely to search the internet, staff will monitor the content of the websites the young people visit.

4.2 Education - Parents/Carers

Each Academy seeks to provide information and awareness to parents and 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 school E-Safety Policy and Acceptable Use Policy.
- The E-Safety Coordinator and Designated Safeguarding Officer 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.

4.4 Education - Governors

Governors 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).

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 Federation 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 regularly monitored.
- The Federation 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 Federation 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 Federation's technical systems and users are made aware of this in the Acceptable Use Agreement.
- 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 Federation's systems and data. These are tested regularly. The Federation infrastructure and individual workstations are protected by up-to-date anti-virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school 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 Federation.

- Users are encouraged to use the secure virtualisation systems for application access.
- Filtered wireless internet is available to users in the Federation.
- In boarding, a monitored, but more relaxed filtering system is used.
- The Academies have a set of clear expectations and responsibilities for all users.
- The Federation adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- 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.

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, but must follow Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment; the personal equipment of staff should not be used for such purposes.
- 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.
- Consideration will be given in each case whether to use a student's full name on a website or blog, particularly in association with photographs.

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

8 Unsuitable/inappropriate activities

The Trust believes that staff should not engage in unsuitable or inappropriate activities in school or outside school when using Academy equipment or systems. 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 Federation provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the Federation:

- Training which includes: acceptable use; social media risks; checking of settings; data protection; 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 community.
- Personal opinions are not to be attributed to the Academy or 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 the Social Media (Employee) Policy which is available on the Federation website.

8.2 User Actions

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from Federation and all other technical systems and could lead to criminal prosecution. Other activities e.g. cyber-bullying, would 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, as defined below, should not engage in these activities in school or outside school when using school 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
	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.

Students are encouraged to report any incidents of misuse to a member of staff or trusted adult immediately. Any reported incidents will be taken seriously by The Federation.

Where bullying is found to have taken place by any means, whether on-site or off-site, including cyber-bullying, robust action shall be taken to protect the wellbeing 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.

- If you feel you are being bullied by email, text or online, do talk to someone you trust.
- Never send any bullying or threatening messages. Anything you write and send could be read by an adult.
- Serious bullying should be reported to a member of staff; in some cases The Academy will inform the police - for example, threats of a physical or 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 bullying people 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. If they are about you, keep them as evidence. If they are about someone else, report them to a member of staff or trusted adult. Do not reply to the sender.

- **Don't** ever give out passwords to your mobile or email account.
- **Remember** that sending abusive or threatening messages is against the law.

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 Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the DSOs at each academy are to be contacted immediately. The contact details for each of the Academies' Lead DSOs and DSOs will be posted appropriately throughout the Academy and all staff are to be made aware of the DSOs at staff briefings on a regular basis and as part of staff induction. In the event that a DSO or LDSO is not immediately available, a member of the Senior Leadership Team is to be alerted at once (in line with the Federation's safeguarding procedures).

The DSO/LDSO/SLT will notify the Headteacher and the Director of Student Welfare (DSW). The DSW is available outside Academy hours on 4355 (internally) or 01522 871355. The DSW will notify the police.

Where necessary the DSW and Head of HR will notify the LADO (Local Authority Designated Officer) accordingly. The Trust's Staff Disciplinary Policy will be invoked if required.

9.2 Other Incidents

It is hoped that all members of the Federation 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 any Academy user has been involved in inappropriate or unsuitable activity, the DSO at the relevant Academy is to be contacted immediately.

- The DSO will escalate the case as described in 9.1 and, if the incident involves a member of staff, the DSW/Head of HR will decide the nature of any investigation, in line with the Trust's Staff Disciplinary Policy.
- Have more than one senior member of staff/volunteer involved in any investigation process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, 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 images of child sexual abuse – 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 computer in question should be isolated. Any change to its state may hinder a later police investigation.

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.

Incidents of misuse involving students will be dealt with in accordance with the Federation Student Behaviour and Discipline Policy.

10 Procedures

This procedure may only be amended or withdrawn by The Priory Federation.

The Priory Federation of Academies Trust
E-Safety Policy

This Policy has been approved by the 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.