Subject	**E-Safety Policy**		
Author	**S Merrick**	Document Review Date	**September 2017**

Version Control

Version	**Date**	**Comments**	**Reviewer**
0.1	10th June 2014	Document Creation	S Merrick
0.2	28th September 2015	Roles Updated & Reviewed	S Merrick
0.3	19th September 2016	Roles Updated & Reviewed	S Merrick

Contents

1. Introduction

This policy applies to all members of the Priory Community School Academy (PCSA) community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are using the PCSA ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such an extent as is reasonable, to regulate the behaviour of students when they are off the school 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 school, but is linked to membership of PCSA. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over the issues covered by the Behaviour Policy.

PCSA will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

2. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within PCSA:

E-Safety Co-ordinator	**Michelle Skelton (Teacher of Computing)**
E-Safety Academy Council Member	**Ken Hanson**
Safeguarding Officer	**Lisa Smith (Lead Safeguarding Officer)**

Academy Council

The Academy Council are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of this policy. This will be carried out by the Academy Council of the Support and Conduct Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Academy Council has taken on the role of E-Safety Academy Council Member. The role of the E-Safety Academy Council Member will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Academy Council Sub Committee (Support & Conduct)

Head of School and Senior Leadership

- The Head of School has a duty of care for ensuring the safety (including the e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Head of School and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

- The Head of School and Senior Leaders are responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head of School and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal safety monitoring role. This is to provide the safety net and also support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Co-ordinator

- leads the E-Safety Committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the relevant body
- liaises with the school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Academy Council meetings
- reports regularly to the Senior Leadership Team

Network & Systems Manager and IT Support Team

The Network & Systems Manager and IT Support team are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required E-safety technical requirements and any other relevant body E-Safety Policy that may apply
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering system 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 the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School, Senior Leaders, and/or the E-Safety Co-ordinator for investigation, action or sanction
- that monitoring software systems are implemented and updated as agreed

Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school E-Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head of School, Senior Leadership Team, and/or E-Safety Co-ordinator for investigation, action or sanction

- all digital communications with students, parents and carers should be on a professional level and only carried out using school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- 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 school 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

Child Protection and/or Safeguarding Officer

Should be trained in E-safety issues and be aware of the potential for serious child protection/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

E-Safety Committee

Members of the E-Safety Committee will assist the E-Safety Co-ordinator with:

- the production, review and monitoring of the E-safety Policy documents
- the production, review and monitoring of the school filtering and requests for filtering changes
- mapping and reviewing the e-safety curricular provision - ensuring relevance, breadth and progression
- monitoring network, Internet and incident logs
- consulting stakeholders - including parents/carers and the students about the E-safety provision
- monitoring improvement actions identified through use of the SWGfL 360 degree safe self review tool

Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- 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 inappropriate materials and know how to do so
- will be expected to know and understand policies of the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet and mobile devices in an appropriate way. PCSA will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website/VLE and information about national/local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in the school (where this is allowed)

Community Users

Community users who access school systems, website or VLE as part of the wider school provision will be expected to agree to a Guest Acceptable Use Policy before using the school systems.

3. Policy Statements

Education - Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across the curriculum. The e-safety curriculum should be broad, relevant, and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety curriculum should be provided as part of Computing lessons and should be regularly revisited
- Key E-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Students should be helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within school and outside school
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices
- In lessons where Internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and the processes are in place for dealing with any unsuitable material that is found in Internet searches
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be audit-able, with clear reasons for the need.

Education - Parents

Many parents and carers have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents Evenings
- High profile events (e.g. Safer Internet Day)
- Reference to the relevant web sites (e.g. www.swgfl.org.uk / www.saferinternet.org.uk / www.childnet.com)

Education - The Wider Community

The school will provide opportunities for members of the community to gain from the schools e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-safety messages targeted towards grandparents and other relatives as well as parents
- The school web site will provide e-safety information for the wider community

4. Training

Training - Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-safety training will be made available for staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies
- The E-Safety Co-ordinator will receive regular updates through attendance at external training events (e.g. from SWGfL, LA, or other relevant organisation)
- The E-Safety Co-ordinator will provide advice, guidance, and training to individuals as required.

Training - Academy Council Members

Academy Council Members should take part in E-safety training/awareness sessions, with particular importance for those who are members of any sub committee involved in technology, E-safety, health and safety, or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, SWGfL, or any other relevant organisation
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies or lessons)

5. Technical - Infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school network infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- PCSA technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and password by the IT Support team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The Network & Systems Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless system, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date antivirus software
- An agreed network is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) on to the school systems

6. Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. However, there are a number of e-safety considerations for BYOD that need to be adhered to:

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises
- Regular audits and monitoring of usage will take place to ensure compliance

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents/carers, and students need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or long term, It is common for employers to carry out Internet searches for potential and existing employees. The school will inform and educate users about these risks.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet (e.g. on social networking sites)
- In accordance with guidance from the Information Commissioners Office (ICO), parents/carers are welcome to take videos and images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published or 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 school policies concerning the sharing, distribution and publication of those images. Those

images should only be taken on school 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 that might bring the individuals or the school in to disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the school website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs

8. Data Protection

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to far greater scrutiny in their care and use of personal data. PCSA has a comprehensive Data Protection Policy which should be referred to for further information.

The school must ensure that:
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date, and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data
- Transfer data using encrypted and secure password protected devices

9. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. PCSA has an Electronic Communications Policy which should be referred to for further information regarding the use of communications technologies.

When using communication technologies the school considers the following as good practice:
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, phone etc) must be professional in tone and context.

- Students should be taught about E-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

10. Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: 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

School staff should ensure that:

- No reference should be made in social media to students, parents/carers, or school staff (unless permitted)
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly by the Safeguarding Officer and E-Safety Committee to ensure compliance with the relevant policies. Further information can be found in the Social Media Policy.

11. Monitoring and Review

The implementation of the this E-Safety Policy will be monitored by the E-Safety Co-ordinator and the E-Safety Committee. This E-Safety Policy has been approved by the Academy Council (Business & Site Committee). It will be reviewed annually.

Signed _____	Date _____
Name _____	**Chair of the Academy Council**

Data Policy Approved - September 2016
The name of the designated person is: Simon Merrick
The Policy is to be reviewed every year and the next review is due in September 2017