SIR ROBERT PATTINSON ACADEMY

E-SAFETY POLICY

Date Reviewed in School:	June 2018
Date Approved by Governors:	**18 June 2018**
Review Date:	June 2021

Introduction

This policy recognises the commitment of the academy to e-safety and acknowledges its part in the academy's overall safeguarding policies and procedures. It demonstrates our commitment to develop a set of safe and responsible behaviours and we recognise our obligation to implement a range of security measures to protect the academy network and school data

It applies to all members of the Sir Robert Pattinson Academy community (including governors, staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers head teachers 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. 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 issues covered by the published Behaviour Policy.

The Academy 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.

Responsibilities

The person in the academy taking on the role of e-safety coordinator is Ms E Allsopp

The Governor with an overview of e-safety is Dr N Appleby.

Responsibilities of the Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor and this is Dr N Appleby. The role of the Safeguarding Governor will include:

- regular contact with the E-Safety Co-ordinator / Officer

Responsibilities of the Senior Leadership Team:

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Deputy head (Safeguarding).
- The SLT are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- Ensure all staff and students agree to the ICT protocol and e-safety which is part of induction of new staff.
- Make appropriate resources, training and support available to all members of the academy to ensure they are able to carry out their roles effectively with regards to e-safety
- Ensure and promote an e-safety culture within the academy
- Ensure adequate logistical support is in place to maintain a secure ICT system

- Liaise with governors
- Ensure policies and protocols are in place to ensure integrity of the academy's information and data assets
- Take every opportunity to help parents understand these issues through a range of methods which may include parents' evenings, newsletters, letters, website / Virtual Learning Environment (VLE) and information about national / local e-safety campaigns / literature.
- The SLT will receive regular monitoring reports from the E-Safety Co-ordinator.

Responsibilities of the E-Safety Coordinator:

- ensures e-safety education is embedded in the curriculum
- promotes e-safety to parents and the community
- take day to day responsibility for e-safety issues and a leading role in establishing and reviewing the school e-safety policy
- ensures that all staff are aware of the procedures that needs to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff on e-safety issues
- liaises with the Local Authority, Local Safeguarding Children's Board and other agencies as appropriate
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to the Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team
- follows the Academy's Behaviour Policy when dealing with any incidents.

Responsibilities of the ICT Technical staff:

- Support the academy in providing technical infrastructure which is secure and is not open to misuse or malicious attack
- Ensure that the academy meets required e-safety technical requirements and any Local Authority Guidance that may apply.
- At the request of the head or e-safety coordinator conduct checks on files, folders any other digital content to ensure policies are being followed
- Ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Apply and update the filtering policy on a regular basis and that its implementation is not the sole responsibility of any single person
- 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
- 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 the E-Safety Coordinator
- Implement and update monitoring systems as agreed in academy policy
- Document all technical procedures and review as appropriate

- Ensure appropriate backup procedures exist so that systems can be recovered in the event of a disaster
- Ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff
- Ensure that the managed service provider is fully aware of the academy e-safety policy and procedures.

Responsibilities of the Teaching and Support Staff:

- Read and understood the 'Code of Conduct for staff, Governor's and Volunteers' and the e-safety policy before using any ICT systems
- Take responsibility for ensuring the safety of sensitive school data and information
- Ensure they are GDPR compliant when sharing data via email
- Have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- Report any suspected misuse or problem to the E-Safety Coordinator
- Ensure that all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- Ensure all digital communication with students is in a professional level and only through academy based systems, never through personal email, texts, mobile phone, social media or any other digital media
- Ensure that e-safety issues are embedded in all aspects of the curriculum and other activities where appropriate
- Ensure that students understand and follow the e-safety and acceptable use policies
- Ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Monitor the use of digital technologies, for example mobile devices, cameras in lessons and other school activities and implement current policies with regard to these devices
- Ensure that in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Be aware that internet traffic can be monitored and traced to individual users. Discretion and professional conduct is essential.
- Maintain a professional level of conduct in their personal use of technology al all times
- Know that staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Responsibilities of the Child Protection Officer:

- 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

Responsibilities of the Students:

- Be responsible for using the academy digital technology systems in accordance with the ICT Protocol (See Appendix 1)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Report all e-safety incidents to appropriate members of staff
- Expect to know and understand policies on the use of mobile devices and digital cameras.
- Know and understand policies on bullying.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the academy's E-Safety Policy covers their actions out of school, if related to their membership of the school

Responsibilities of the 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 and support the academy in promoting e-safety. Parents and carers will be encouraged to support the Academy in promoting good e-safety practice.

- Follow academy guidelines on the use of digital and video images taken at school events
- Have access to parents' sections of the website / VLE and on-line student records
- Read, understand and promote the protocol
- Consult with the academy if there are any concerns about their child's use of technology
- Follow academy guidelines with regards to their children's personal devices in the Academy (where this is allowed)

Responsibilities of external users and visitors (e.g.: community learning)
Community Users who access school systems as part of the wider Academy provision will be expected to sign a Community User AUA before being provided with access to school systems.

- Take responsibility for liaising with the academy in appropriate use of academy ICT equipment and content
- Ensure they follow the acceptable use policy.

Managing and safeguarding the ICT system

The Academy will ensure that access to the academy IT system is as safe and secure as reasonably possible.

Servers and other key hardware are located securely; the wireless network is protected by a secure log on which prevents unauthorised access. Only technical staff can download and install software.

Protecting Academy data and information

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation May 2018.
- Student Data Retention. The ICT Team will archive data from login accounts and retain this for 5 years.

Authorising access

- All staff must read the 'Code of Conduct for staff, Governors and Volunteers' before using any Academy ICT resource.
- The Academy will maintain a current record of all staff and students who are granted access to Academy ICT systems.
- Access to the ICT resources and/or the internet will be withdrawn should the system be used inappropriately.
- Access to the school system for all users is password protected. This password is regularly required to be changed.
- Staff, students, parents and Governors can access the system via direct login when on school site or via a web portal remotely. Sixth form students can also logon to their accounts via their own devices in school which will also have some form of filtering.
- Remote working is available to staff and is provided by an industry leading SSL VPN appliance. Ensuring a safe experience.

Managing filtering

- The Academy will work in partnership with external consultants in monitoring all content when accessing the internet or other ICT related tasks. Reports will be available the leadership team.
- If staff or students discover an unsuitable site, it must be reported to the ICT Coordinator.
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Assistant Headteacher responsible for Safeguarding will regularly access Securus software which monitors all on and offline content and deal with any issues according to, in the case of students the Behaviour Policy and in the case of staff the code of conduct including disciplinary.
- The above policies also apply to the use of Apps for Windows, Android and Apple.

Information system security

- The Academy has implemented a Gateway Security Device and Web filter. This is maintained by an external company.
- The Academy Wireless system is secured by the gateway Security Device
- Academy ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- System updates, patches and hotfixes are kept up to date
- System monitoring will be maintained up to date
- Encryption will be deployed on staff laptops
- Every desktop enabled system will be monitored by Securus Software for Student Safety
- Data is backed up in real time and sent off site for disaster recovery, in an encrypted format
- Access to personal, private or sensitive information and data is restricted to authorised users only

Using the internet

Why internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The Academy has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

- The Academy internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate internet content

- Schools should ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Downloading of content

- Downloading of files, such as torrents, films and music is mostly illegal and in breach of copy write law and can lead to sanctions in line with the school behaviour policy. This should not be done via the Academy internet.
- Unauthorised files should not be downloaded at home and brought into the school.

Using email

- All students and staff have a network account and individual email address.
- Students must immediately tell a teacher if they receive offensive e-mail. The member of staff will then alert the IT team and where necessary the Assistant Headteacher in terms of safeguarding.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully in the same way as a letter written on Academy headed paper.
- The forwarding of chain letters/emails is not permitted.
- An Email disclaimer will automatically be added to any Academy email
- Emails are scanned for Virus and unsuitable or dangerous content
- Only Academy email accounts maybe used by staff to communicate to students and parents

Using images, video and Social Media

Publishing content and the Academy web site

- The contact details on the Web site should be the Academy address, e-mail, telephone and fax number. Staff or students' personal information will not be published although pictures of students may be accessible if agreed by the student according to the General Data Protection Regulation.
- Jorge Thomas will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing student's images and work

- Photographs that include students will be selected carefully and only shared when consent is granted by the student.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.

Using mobile phones

- Mobile phones are not permitted to be used around the academy site apart from in designated areas by staff or sixth form. Members of the Senior Leadership Team will be exempt from this when responding to a call on their school mobile phone.
- Mobile phones are not to be used to record take photos of any other member of the academy staff or student whilst on the Academy site or during an Academy authorised event and then used in such a way as to cause upset to that member.

Using other Technology

- Emerging technologies such as mobile devices, laptops, tablets etc., will be examined for educational benefit and a risk assessment will be carried out before use in the Academy.
- Wireless network will be available to students for mobile use only at set areas of the school.
- The use of mobile technology to send abusive or inappropriate text messages or email is forbidden as is the videoing or photographing of others without permission.
- Bypassing of the filtering and use of Proxy Sites is strictly prohibited. This will be monitored and reported

E-Safety

E-Safety at SRPA depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and taught lessons covering e-safety.
- Sound implementation of e-safety policy in both administration and curriculum, including secure Academy network design and use.
- The use of web filtering and Securus Student Safeguarding Software to monitor and filter student activity on the internet and Academy Desktop Environment, regardless of device (tablet, laptop, phone, PC, VDI or remote access).

Introducing the e-safety policy

- Students will be informed that network, desktop environment, BYOD and Internet use will be monitored while used in the Academy or via remote access.
- Staff will be made aware of the Academy's policy on induction and will be referred to the ICT protocol.

When dealing with students, staff should

- Not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites
- Only use equipment e.g. mobile phones, provided by organisation to communicate with students, making sure that parents have given permission for this form of communication to be used
- Only make contact with students for professional reasons and in accordance with any organisation policy

- Recognise that text messaging is rarely an appropriate response to a student in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible
- Not use internet or web-based communication channels to send personal messages to a child/young person
- Ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum

Enlisting Parent Support

- Parents' attention will be drawn to the Academy E-Safety Policy in newsletters, the Academy brochure and on the Academy Web site.
- Parent Information evenings will be held to educate parents on E-safety.

Cyber bullying

- The use of mobile and or electronic devices to intentionally or unintentionally cause harm can have a devastating impact on victims.
- Any suspected cases of cyber buying should be reported through the normal Academy system.
- Screen captures of suspected incidents are taken by Securus and these images where appropriate, are reviewed by the Deputy Head teacher for Safeguarding.

Dealing with an e-safety incident

- Should a student be concerned in relation to e-safety, they should report this concern to their teacher, this concern can then be either addressed there and then or can be escalated to the Designated Safeguarding officer.
- Should the incident warrant, an investigation will be undertaken by the Designated Safeguarding Officer and relevant agencies informed.
- The following events are likely to result in disciplinary action:
    - Repeated posts, comments, publishing of images that cause distress
    - Posting of inappropriate images of other members of the academy
    - Publishing or commenting on another member of the academy in a derogatory manner or in such a way that brings distress

E-SAFETY POLICY

The E-Safety Policy is part of the Academy Development Plan and relates to other policies including:

- ICT Protocol
- Behaviour Management including Anti-Bullying
- Safeguarding
- Data Protection

Appendix 1

ICT Protocol

Name:_____ **Form**:_____

As a student, when using the school network and other ICT equipment, I will:

- only log on using my own username and password;
- make sure that I keep my password secret;
- not attempt to alter any computer settings, including background images;
- not attempt to download, upload or otherwise bring onto the school network any programs or files that may contain hidden programs;
- not attempt to find files on the school network that do not concern me;
- only use the computers for school work or homework;
- report any faults straight away to a teacher or ICT technician;
- not take photographs or video of anyone without their permission;
- not deliberately seek out inappropriate or offensive material or seek to bypass the school Internet filters;
- report to my teacher any inappropriate material that I find accidentally this includes any material of a violent, dangerous, racist or inappropriate sexual nature;
- only access games sites specifically directed by my teacher;
- never publish personal details about myself or other people;
- not use chat rooms, instant message type applications or social networking sites;
- refrain from using offensive language in emails;
- not use the school email system to send messages that are likely to upset others;
- always report any unpleasant emails that I receive to a teacher;

Signed_____ Date_____

As a parent I will:

- confirm that my son/daughter has read the attached terms of acceptable use and agrees to abide by them when using the ICT facilities available in school.
- understand that school staff may check a student's files and emails as well as monitoring the Internet sites that they visit.
- understand that failing to comply with these rules may result in sanctions being applied to their account, possibly restricting access to facilities for a period of time and that this may impact their learning.
- understand that the academy may take action as a result of digital communication which brings the academy, staff or students distress.

Signed_____ Date_____

As the academy we will:

- provide suitable ICT facilities;
- provide technicians to support students with technical issues;
- provide a filtering service to reduce the access to offensive or inappropriate material;
- block access to social media sites on school equipment.

ICT Teacher Signed_____ Date_____