SIR ROBERT PATTINSON ACADEMY

E-SAFETY POLICY

Date Reviewed:	March 2024
Date Approved by Trustees:	**5 February 2024**
Review Date:	December 2026

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 Academy data.

It applies to all members of the Sir Robert Pattinson Academy community (including Trustees, 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 the Academy.

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our Academy aims to:

- Have robust processes (including filtering and monitoring systems) in place to ensure the online safety of students, staff, volunteers and governors.
- To limit children's exposure to the 4 key categories of risk (described below) from the Academy's IT systems but which also allows learning to proceed, this will be reviewed regularly for effectiveness.
- Protect and educate the whole Academy community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Set clear guidelines for the use of mobile phones for the whole Academy community.
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-

consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The Academy will offer a proactive, sympathetic and supportive response to students who are the victims of bullying. The exact nature of the response will be determined by the **particular student's individual needs** and may include:

- Immediate action to stop the incident and secure the child's safety;
- Positive reinforcement that reporting the incident was the correct thing to do;
- Reassurance that the victim is not responsible for the behaviour of the bully;
- Informing parents at the earliest opportunity;
- Strategies to prevent further incidents;
- Sympathy and empathy;
- Counselling;
- Befriending /creation of a support group;
- Extra supervision/monitoring;
- Peer mediation/peer mentoring;
- Adult mediation between the perpetrator and the victim (provided this does not increase the victim's vulnerability);
- Arrangements to review progress.

Social networking websites are sometimes used for bullying and any threats made on such a site and acted on in the Academy will be classed as pre-meditated and are likely to result in a more severe sanction. It should be acknowledged that it can be very difficult for the Academy to take action on cyber bullying which has occurred outside of Academy time, within the behaviour policy.

Responsibilities

The person in the Academy taking on the role of E-Safety Coordinator is Mrs R Gilbert.

The Trustee with an overview of E-Safety is Mr L Harman.

Responsibilities of the Trustees:

Trustees 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 Board of Trustees receiving regular information about E-Safety incidents and monitoring reports. A member of the Board of Trustees has taken on the role of Safeguarding Governor and this is Mr L Harman. 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 Academy 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 the Academy 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 Trustees
- 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 Academy 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 Academy 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 Trustee to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to the 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 Academy technical staff
- Ensure that the managed service provider is fully aware of the Academy E-Safety policy and procedures.
- To conduct and respond to the actions of external network reviews.

Responsibilities of the Teaching and Support Staff:

- Read and understood the 'Code of Conduct for staff, trustees and volunteers and the E-Safety policy before using any ICT systems
- Take responsibility for ensuring the safety of sensitive Academy 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 Academy 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 Academy 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 at 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.

- Monitor student ICT usage within the classroom via Impero Console. Use realtime live monitoring to student computers, review violations and escalate concerns to safeguarding and IT support teams.

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/Acceptable Use 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 the Academy and realise that the Academy's E-Safety Policy covers their actions out of the Academy, if related to their membership of the Academy

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 Academy 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 Academy systems as part of the wider Academy provision will be expected to sign a Community User AUA before being provided with access to Academy systems.

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

Online Safety Group

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- Deputy Safeguarding Leads
- Data Protection Officer
- ICT Network Manager
- Business Manager

Members of the Online Safety Group will assist the DSL with:

- the production/review/monitoring of the Academy Online Safety Policy/documents
- the production/review/monitoring of the Academy filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the Academy online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

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 1 year.

Authorising access

- All staff must read the 'Code of Conduct for staff, trustees 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 Academy system for all users is password protected. This password is regularly required to be changed.
- Staff, students, parents and Trustees can access the system via direct login when on Academy site or via a web portal remotely. Sixth form students can also login to their accounts via their own devices in Academy which will also have some form of filtering.
- Remote working is available to staff and is provided by a secure remote desktop gateway. Ensuring a safe experience over a secure encrypted connection to the Academy servers.
- All staff and students are required to set up multi-factor authentication to access Academy Microsoft office apps and remote access. All teachers and students authenticate when connecting to systems externally and support staff a key members authenticate on all occasions for additional layer of security.

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 team.
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. The Academy uses Smoothwall web content filtering, it is designed to help monitor internet browsing, block and alert about activity which may pose risks to students.
- Deputy Headteacher, safeguarding teams and IT staff responsible for Safeguarding will regularly access Smoothwall monitor and Impero 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. Both tools alerts in real time and captures activity that may indicate a risks to students.
- The above policies also apply to the use of Apps for Windows, Android and Apple devices.
- The Academy manages access to content across its systems for all users and on all devices using the Academy's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for academies and colleges and the guidance provided by The UK Safer Internet Centre (UKSIC) published Appropriate Filtering and Monitoring Definitions.

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 Impero Software and Smoothwall monitor for Student Safety
- Data is backed up daily, weekly and monthly 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

Monitoring

The Academy has monitoring systems (Smoothwall Monitor and Impero) in place to protect the Academy, systems and users:

- The Academy monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted upon and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

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

- Academies 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 Academy behaviour policy. This should not be done via the Academy internet.
- Unauthorised files should not be downloaded at home and brought into the Academy.

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 Deputy 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
- Students are not permitted to email their peers.
- All external email traffic involving students are moderated through the IT support department and are only approved if appropriate and deemed of educational value.
- Any suspicious emails found are to be reported via the ‘Report Phishing’ button found within Outlook. Staff are expected to carry out training to identify phishing and spam emails. Staff vigilance will be tested through the academic year through simulated phishing campaigns.

Using images, video and Social Media

Publishing content and the Academy website

- The contact details on the website should be the Academy address, e-mail and telephone 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.
- The IT support team will take overall editorial responsibility and ensure that content is accurate and appropriate.

Academy staff should ensure that:

- Photographs that include students will be selected carefully and only shared when consent is granted by the parent.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- No reference should be made in social media to learners, parents/carers or Academy staff.
- They do not engage in online discussion on personal matters relating to members of the Academy community.
- Personal opinions should not be attributed to the Academy.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media
- When official Academy social media accounts are established, there should be:
    - a process for approval by senior leaders
    - clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
    - a code of behaviour for users of the accounts
    - systems for reporting and dealing with abuse and misuse
    - understanding of how incidents may be dealt with under Academy disciplinary procedures.

- Personal use is described in the staff code of conduct
- The use of public social media is monitored

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the Academy it must be made clear that the member of staff is not communicating on behalf of the Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the Academy are outside the scope of this policy
- Where excessive personal use of social media in the Academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The Academy permits reasonable and appropriate access to personal social media sites during Academy hours

Monitoring of public social media

- As part of active social media engagement, the Academy may pro-actively monitor the Internet for public postings about the Academy.
- The Academy should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the Academy on social media we will urge them to make direct contact with the Academy, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the Academy complaints procedure.

Academy use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the Academy is unable to resolve, support may be sought from the Professionals Online Safety Helpline.

The social media policy provides more detailed guidance on the Academy's responsibilities and on good practice.

Youtube

- The Academy enforces the use of restricted mode version of Youtube to ensure students are safeguarded from harmful content. Often videos are wrongly flagged as inappropriate and can unnecessarily blocked, deeming Youtube an unreliable teaching and learning resource. Staff are required to regularly test videos for blocking.

Using mobile phones

- Use of personal devices for Academy use is defined in the BYOD, acceptable use policy and staff handbook. Personal devices commissioned onto the Academy network are segregated effectively from Academy-owned systems.
- the use of devices on trips/events away from the Academy is clearly defined and expectation are well-communicated.
- 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, House teams and other staff members with key responsibilities will be exempt from this when responding to Academy matters.
- 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.
- Personal devices such as mobile phones can be used for work purposes. Staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.

- Staff will use mobile phones for the purpose of adhering to security policies clearly set out in the BYOD and AUP. This can include multifactor authentication to Office 365 when at home and in the Academy and Office 365 apps. The Academy takes ownership of its data through Company Intune Policies. (Company Portal app) thus adhering to the Academy Data Protection Policy.
- Staff will use mobile phones for the purpose of adhering to security policies clearly set out in the Student ICT Protocol or AUP. This can include multifactor authentication to Office 365 when at home.

Using other Technology

- Any emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy.
- A wireless network will be available to students for mobile use only at set areas of the Academy.
- 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
- When devices are not owned by the Academy, users must adhere to the Bring your own device (BYOD) policy and Acceptable Use Policy (AUP) policies.

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 the E-Safety Policy in both administration and curriculum, including secure Academy network design and use.
- The use of Smoothwall web filtering and Impero Software to monitor and filter student activity on the internet and Academy Desktop Environment, regardless of device (tablet, laptop, phone, PC 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.
- Online training is offered to parents/carers to support their child/ren.

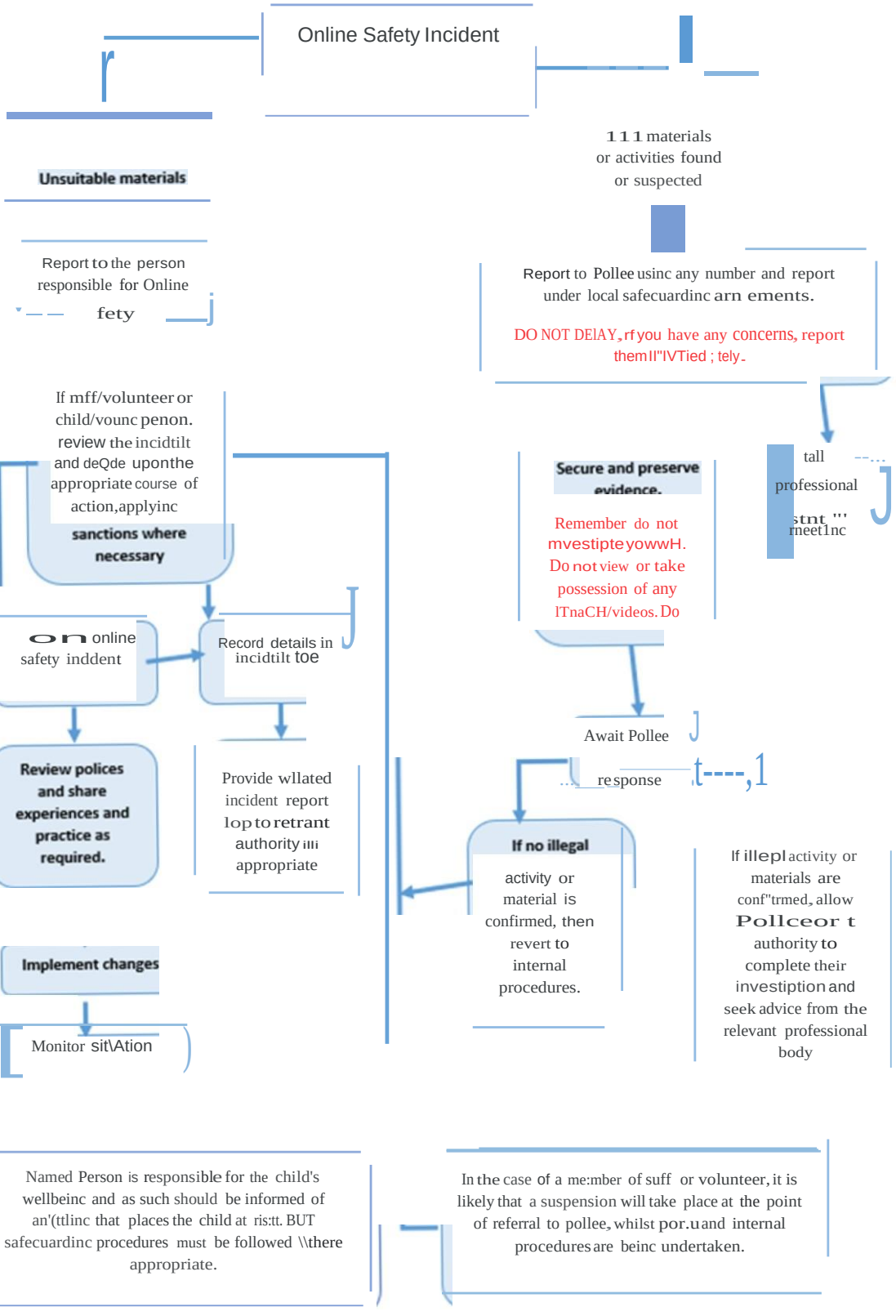
- Regular opportunities for engagement with parents/carers regarding online safety issues are offered through awareness workshops, parent/carer evenings etc
- Students are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant e-safety web sites/publications on the Academy website

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 Smoothwall monitor and Impero and these images where appropriate, are reviewed by the Deputy Head teacher for Safeguarding.

Dealing with an E-Safety incident

- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- 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/Lead.
- Should the incident warrant, an investigation will be undertaken by the Designated Safeguarding Officer/Lead 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


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online fety
111 materials or activities found or suspected
Report to Pollee usinc any number and report under local safecuardinc arn ements.
DO NOT DElAY, rf you have any concerns, report them II"IVTied ; tely.
tall professional
stnt "' rneet1nc
If mff/volunteer or child/vounc penon. review the incidtilt and deQde uponthe appropriate course of action,applyinc sanctions where necessary
Secure and preserve evidence.
Remember do not mvestipte yowwH. Do not view or take possession of any lTnaCH/videos. Do
on online safety inddent
Record details in incidtilt toe
Await Pollee response
Review polices and share experiences and practice as required.
Provide wllated incident report lop to retrant authority illi appropriate
If no illegal activity or material is confirmed, then revert to internal procedures.
If illepl activity or materials are conf"trmed, allow Pollceor t authority to complete their investiption and seek advice from the relevant professional body
Implement changes
Monitor sit\Ation
Named Person is responsible for the child's wellbeinc and as such should be informed of an'(ttlinc that places the child at ris:tt. BUT safecuardinc procedures must be followed \\there appropriate.
In the case of a me:mber of suff or volunteer, it is likely that a suspension will take place at the point of referral to pollee, whilst por.u and internal procedures are beinc undertaken.

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
- Child Protection
- Data Protection
- Bring your own device (BYOD)
- Acceptable Use Policy
- Artificial Intelligence Policy

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online 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 longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- **the Academy may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.** Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**
- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on Academy devices. The personal devices of staff should not be used for such purposes**
- 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). 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 *learners* in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Academy policies concerning the sharing, storage, distribution and publication of those images

- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with the Online Safety Policy
- **learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- **written permission from parents or carers will be obtained before photographs of learners are taken for use in the Academy or published on the Academy website/social media.** (see parents and carers acceptable use agreement in Appendix 1). Permission is not required for images taken solely for internal purposes
- **parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the Academy data protection policy**
- **images will be securely stored in line with the Academy retention policy**
- learners' work can only be published with the permission of the learner and parents/carers.

Appendix 1

ICT/ACCEPTABLE USE PROTOCOL

Name:_____
Form:_____

Digital technologies have become integral to the lives of children and young people, both within the Academy and outside the Academy. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk. The Academy will have good access to digital technologies to enhance students' learning and will, in return, expect the *learners* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use Academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy's systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I will not use my own mobile phone in the Academy.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any Academy device, nor will I try to alter computer settings.
- I will not use social media sites while using the Academy system.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be online bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the Academy network/internet, detentions, suspensions/exclusions, contact with parents/carers and in the event of illegal activities involvement of the police.

Please complete the section below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to Academy systems and devices.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to Academy systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy's systems and devices (both in and out of the Academy)
- I use my own devices in the Academy (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the Academy in a way that is related to me being a member of this Academy e.g. communicating with other members of the Academy, accessing Academy email, VLE, website etc.

Name of Learner: .....
R2L: .....
Signed: .....
Date: .....