Rowley Park

Primary Academy

Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed with the Head of School, Executive Headteacher, Designated Safeguarding Lead (and deputy) and other staff including technical staff and teachers.

This Online Safety policy was approved by the Academy Council on:	
The implementation of this Online Safety policy will be monitored by the:	Helen Smith (DSL/Subject lead)
Monitoring will take place at regular intervals:	Annually
Academy Councillors will receive a review on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	February 2021
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Kate Tewley – Executive Headteacher LADO – at Staffordshire Safeguarding board Staffordshire Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys / questionnaires of staff, pupils and parents/carers.

Scope of the Policy

This policy applies to all members of Rowley Park Academy (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of schools digital technology systems, both in and out of school.

The school 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 Online Safety behaviour that take place out of school.

Roles and Responsibilities

Academy Councillors

Academy Councillors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Councillors in their Monitoring visits.

Computing Lead/DSL

Helen Smith takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies including training and advice for staff, liaising with technical staff and acting on online safety concerns/misuse.

Network Manager / Technical staff

The Network Manager and technical Staff are responsible for ensuring that filtering is effective, that the schools technical infrastructure is not open to misuse or malicious attack and that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. They ensure that school meets required online safety technical requirements as well as support the day to day technical needs of the school.

Teaching and Support Staff

All teaching and support staff have a responsibility to ensure that they have read, understood and signed the Staff Acceptable Use Agreement (AUA) and report any suspected misuse or problem to the *DSL* (Helen Smith).

Designated Safeguarding Lead (Helen Smith)

The DSL is aware of online Safety issues and the potential for serious child protection / safeguarding issues including: sharing of personal data, accessing illegal or inappropriate material, inappropriate on-line contact with adults, potential or actual incidents of grooming and online bullying.

Pupils:

Pupils are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement.

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.

Teaching and learning

Rowley Park Academy believes that the internet is an essential resource in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. The education of pupils in online safety and digital literacy is an essential part of the school's online safety provision, helping and supporting pupils to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages in lessons. Pupils will:

- Be taught how to use the internet safely and appropriately
- Shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content:

- The school will ensure that materials used complies with copyright law.
- Pupils will be taught the importance of evaluate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content by using the Child Exploitation and Online Protection Centre (CEOP) "Report Abuse" icon
- Pupils will know what to do if they experience any issues whilst online.

Supporting Parents / Carers

To support parents and carers with their understanding of online safety risks and issues, the school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, texts
- Parents / Carers workshops
- Reference to the relevant websites e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Managing internet Access:

- Rowley Park Academy's technical systems will be managed in ways that ensure that the meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Virus protection will be updated regularly.
- Internet access is filtered for all users. The school has provides enhanced / differentiated user-level filtering.
- Internet systems are regularly monitored users are made aware of this in the Acceptable Use Agreement.
- Systems are in place for users to report any actual / potential technical incident / security breach to the relevant person (DSL – Helen Smith).
- AUA is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Written permission from parents /carers is obtained before photographs of pupils are published on the school website / Twitter/ local press and photographs will be chosen carefully.
- Videos and digital images of their children at school events by parents should for their own personal use. These images should not be published / made publicly available on social networking sites.

- Staff are allowed to take digital / video images to support educational aims using **school owned technologies**, but must follow school's procedures concerning the sharing, distribution and publication of those images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection (see Victoria Academies Trust GDPR Data Protection Policy)

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation**.** **GDPR Policy**

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. Memory sticks and other removal media is not permitted.
- Transfer data using encryption and secure password protected devices.

Communication

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. *These communications may only take place on official (monitored) school systems.* ***Personal email addresses, text messaging or social media must not be used for these communications.***

Social Media

Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party will be dealt with in line with Victoria Academy Trust Disciplinary Policy.

For further information see Social Media Policy.

Dealing with unsuitable / inappropriate activities

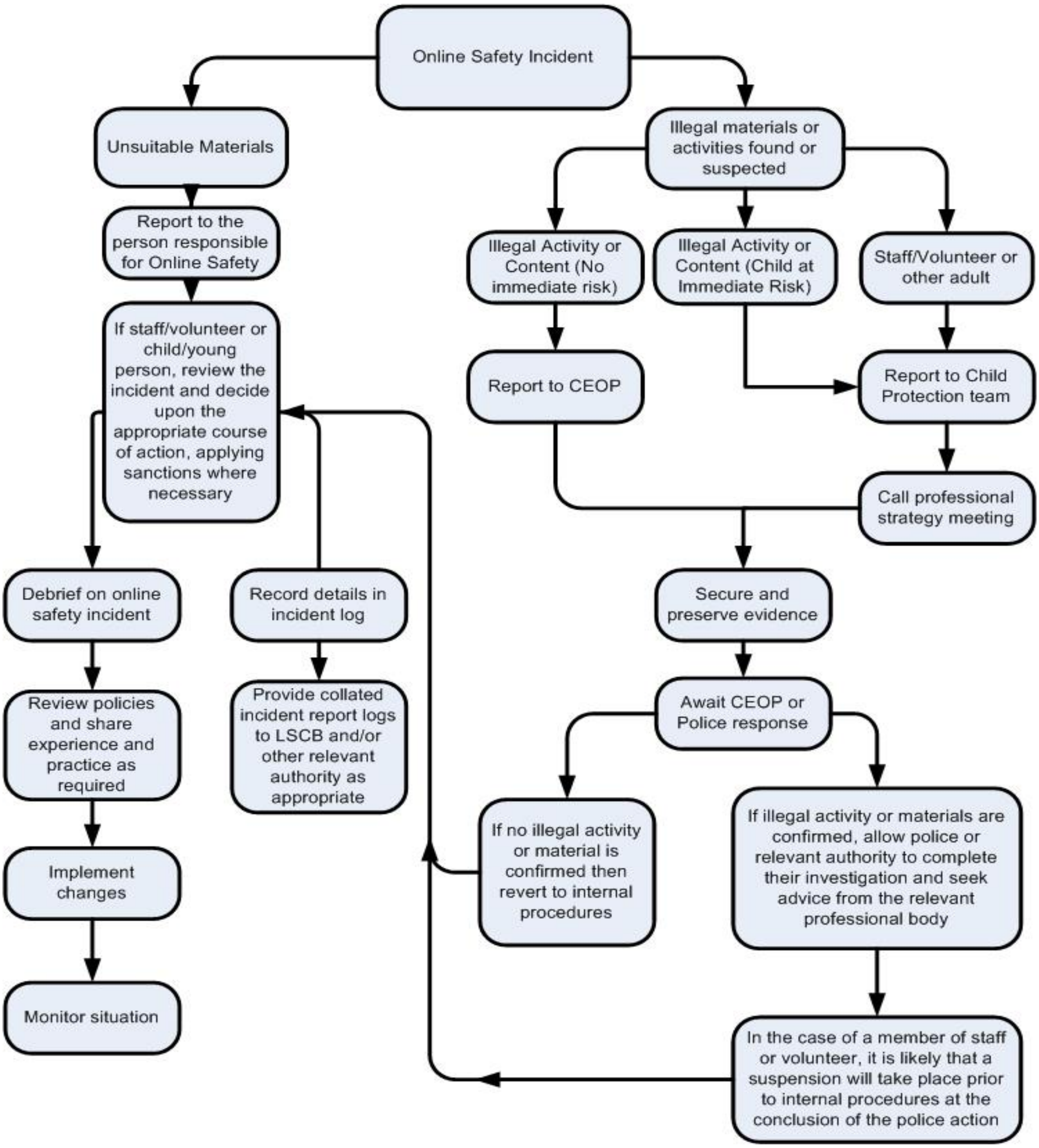
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. All other breaches of policy would be dealt with in line with Victoria Academy Trust Disciplinary Policy.

Responding to serious incidents of misuse

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

All members of the school community will be responsible users of digital technologies and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
- Once this has been completed and fully investigated the Head of School will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the Trust /LADO
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

REPORTING

All online safety concerns, must first be reported to an adult who will then complete an E-Safety incident log report. These forms can be found in Phase Leaders Behaviour logs, the school office and outside the Training room. They are also available on TEAMs. The incident log should then be taken to either Helen Smith (DSL/Computing lead) or in her absence Annika Beaumont (Deputy DSL/Head of School). If neither are available a member of SLT should be handed the form. Any relevant incidents will be recorded using the online safeguarding system Safeguard. Appropriate action in line with relevant school policies will be taken and recorded.

Appendix

Acceptable User Agreement - Key Stage 1

Acceptable User Agreement - Key Stage 2

Acceptable User Agreement – Staff

E-safety Incident form

E-safety Log

Links

This policy should be used in conjunction with:

- Safeguarding and Child Protection Policy
- Social Media policy
- Staff Code of Conduct
- Behaviour for Learning Policy
- Anti-Bullying policy
- Victoria Academies Trust GDPR policy
- Disciplinary Policy

Key Stage 1 Acceptable Use Agreement

I understand that this is how we stay safe when we use the computer or iPads:

S I will ask an adult if I want to use the computer or iPad

S I will only use activities or apps that the adult has told me I can use

S I will look after the computers and iPads

t I will ask for help from an adult if I am not sure what to do or something has gone wrong

t I will tell an adult straight away if I see something on the screen that upsets me

S I know teachers will check the computers and iPads to make sure I am safe

I understand that if I break the rules, I might not be allowed to use the computers or iPads.

Key Stage 2 Acceptable Use Agreement

I understand that this is how we use technology at Rowley Park Academy:

s I am aware that some websites, games and social media sites have age restrictions and that I should respect this.

s I will not make, send or post anything that is likely to upset other children or adults and I will not post anything without their permission.

s I know that RPA will monitor my use of ICT in school.

s I will not give my usernames and passwords away and I will tell my teacher if I think someone knows it.

s I will not deliberately type or search for anything that is banned, unkind or inappropriate. If something appears accidentally, I will tell an adult straight away.

s I will take care of all equipment.

m I will not reveal any personal information about me to any strangers (e.g. full name, home address, age, telephone number)

m I will be polite and not use nasty words when typing or talking to my friends.

m If someone tries to speak to me online who I do not know, I will not reply and tell an adult.

a If I am not sure about an email attachment, picture or message, I will tell an adult straight away.

a I will not click on pop ups that may appear on my screen.

a I will not attempt to download and/or install any unapproved software or resources from the Internet.

r I know that not all information I see online is true, I will make sure that I check more than one website to check it's real.

If I am worried or upset by something I see on the computer or any other ICT equipment, I will tell an adult straight away.

I understand that:

- I must use school ICT in a responsible way to ensure that there is no risk to me, other school users or school systems and security
- that only equipment owned by the school will be used on the school site
- any mobile devices that are not **school owned** must be stored in the school office and not used on the school site (Year 5 & 6 who walk home alone)

Signed:

Staff Acceptable User Agreements

For my professional and personal safety:

- I understand that my use of the school digital technology will be monitored.
- I understand that this agreement applies to the use of school technologies (laptops, iPads etc.) out of school, and to transfer data out of school.
- I understand that school technology systems are intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username or password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

My professional communications and actions on Academy owned technology:

- I will not copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take/publish images of others I will do so with their permission in accordance with school's policies, **using only school equipment.**
- I will only use social networking sites in line with school policy (Twitter).
- I will only communicate with pupils and parents/carers using school systems (Showbie, Twitter etc.) Any such communication will be professional in tone.

Safe and Secure

- I will not use personal email addresses for academy communications.
- I will not open hyperlinks in emails or attachments unless the source is trusted, or I have concerns about the validity of the email.
- I will not try to upload/download/access materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not try to bypass filtering/security systems.
- I will not try to install or attempt to install programs of any type or alter computer setting without first checking with ICT technician.
- I will not disable or cause damage to Academy equipment.
- I will only transfer data in line with school GDPR policy. Where digital personal data is transferred outside of secure local systems, it must be encrypted.
- I understand that data protection policy requires that staff/pupil data is kept private and confidential (always on a password protected device).
- I understand that portable storage devices are not permitted.
- I will immediately report any faults or damage to school equipment or software.

Responsibilities

- I understand that this AUA applies not only to my work and use of school digital technology equipment in school but off site also and my use of personal equipment on site or in situations relating to my employment by the school.
- I understand that if I fail to comply, may result in action in line with the Trust Disciplinary Policy.

I have read and understood the above and agree to use technology within these guidelines.

Staff/volunteer: ……………………………………………………………………………

Signed: ……………………………………………………………………………

Date: ……………………………………………………………………………

E-safety incident form

Date: ____

Concern raised by: ____

Pupils/staff involved: ____

Class: ____

Concern/incident (including where it took place):

Member of staff completing this form:______________________________

Action:

Outcome (SLT to complete):

Signed:

E-safety Incident log

Date	Pupils	Class