Rowley Park
Primary Academy

E-safety Policy 2024

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed with the Headteacher, Designated Safeguarding lead, Computing lead and Trust staff including technical staff.

This Online Safety policy was approved by the Academy Council on:	Date:
The implementation of this Online Safety policy will be monitored by the:	Designated Safeguarding Lead (Helen Smith)
Monitoring of filtering systems will take place at regular intervals:	Monthly
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:	September 2025
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Headteacher Chair of Academy Council LADO – at Staffordshire Safeguarding board Staffordshire Police

The school will monitor the impact of the policy using:

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

This policy is based on our school values of:

Unity Integrity Courage Curiosity Excellence

and is underpinned by the three main principles of:

BE READY	BE RESPECTFUL	BE SAFE
This principle is in reference to the children's attitude and expectations to learning.	**This principle is in reference to the children's attitudes and behaviours towards others.**	**This principle is in reference to the children's behaviours**
READY TO LISTEN, READY TO LEARN, READY TO BE LEADERS	RESPECTFUL ATTITUDE, RESPECTFUL WORDS, RESPECTFUL ACTIONS	SAFE CHOICES, SAFE ACTIONS, SAFE SPACE

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.

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education – remove if not applicable, see section 4]
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Academy Councillors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, 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

Roles and Responsibilities

Academy Council

Academy Councillors are responsible for the approval of the Online Safety Policy, for reviewing the effectiveness of the policy and holding the Headteacher accountable for its implementation. This will be carried out by the Councillors in their Monitoring visits. They will ensure all staff undergo safeguarding training and receive regular e-safety updates to enable them to understand the expectations, roles and responsibilities around monitoring and filtering. This will ensure they have the relevant skills and knowledge to effectively safeguard children. The Academy Council will ensure children are taught how to keep themselves and others safe, including keeping safe online. They will also:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems;
- Review filtering and monitoring provisions at least annually;
- Block harmful and inappropriate content without unreasonably impacting teaching and learning;
- Have effective monitoring strategies in place that meet their safeguarding needs

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Designated Safeguarding Lead – DSL (Helen Smith)

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and AC to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Trust network manager and tech support to make sure the appropriate systems and processes are in place
- Working with the headteacher, network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Positive Relationships and Behaviour Policy
- Updating and delivering staff training on online safety Liaising with other agencies and/or external services if necessary
- Providing regular reports/feedback on online safety in school to the headteacher and/or AC
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Head of IT networks/ Technical staff

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (AUA) and ensuring that pupils follow the school's terms on acceptable use (Pupil AUAs)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by completing the E-safety incident form
- Following the correct procedures by [through Tracy Jones] if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Positive Relationships and Behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

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.

They are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (KS 1 and KS 2 AUA)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet
- School website links - **https://www.rowleyparkacademy.org.uk/community-and-wellbeing-support-links-f-z/**

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on the AUA.

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 technology safely and respectfully (including keeping personal information private)
- Be taught a range of ways to report concerns about content and contact
- Shown how to publish and present information to a wider audience

By the **end of KS 2**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Our curriculum teaches about the safe use of social media and the internet through PSHE and computing lessons. Our PSHE theme of Healthy me and Relationships has a strong focus on online safety but all lessons involving internet use have a element of e-safety taught. Monitoring of e-safety logs and concerns raised, ensures that we are able to adapt the curriculum to meet the needs of the children.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children.

Supporting Parents / Carers around online safety

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

- Sharing local/national e-safety concerns through texts, letters etc
- Providing useful information links on the school website for supporting e-safety issues
- Safeguarding spotlights through Headteacher's newsletters
- Parents / Carers workshops
- Reference to the relevant websites e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Our PSHE overview is available for parents on the school website, as is this e-safety policy and other safeguarding policies.

If parents/carers have any queries of concerns in relation to online safety, these should be raised in the first instance with a member of the safeguarding team (Family support mentor, DSL, Headteacher). They can also raise concerns with any member of staff.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Positive Relationships and Behaviour Policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils (as part of their PSHE and computing lessons), explaining the reasons why it occurs, the forms it may take and what the consequences can be.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Positive Relationships and Behaviour Policy and our Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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.

Examining electronic devices

Pupils are only permitted to bring a mobile phone into school in Years 5 and 6. In these instances, the mobile phone must be handed to the class teacher on entry to school, switched off and securely stored in the school office. It will remain here until the end of the school day when it will be returned to the pupil as they leave school.

However, the headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds (after speaking with the Headteacher) for suspecting any of the above, they will also (alongside the Headteacher):

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Rowley Park Academy recognises that AI has uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Rowley Park Academy will treat any use of AI to bully pupils in line with our Positive Relationships and Behaviour Policy and our Anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable use of the internet in school

All pupils, staff (including temporary staff) and other stakeholders who have access to the school's ICT systems and internet are expected to sign an Acceptable User Agreement (AUA). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, Academy Councillors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – (strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters)
- Staff will not use external hard drives (including memory sticks) in school devices
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software (this will be undertaken by the technology support team prior to the device being provided to staff)
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 4.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Head of IT networks (Richard Barnet) or school technology support team (Tracy Jones).

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on:

- Positive Relationships and Behaviour Policy
- Anti-bullying Policy
- Acceptable User Agreements
- Safeguarding and Child Protection Policy

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct, Grievance Policy, Disciplinary Policy, Low Level Concerns Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

School will use the flow chart below when responding to an incident of misuse.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Academy Councillors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

The school also receives a monthly report raising potential safeguarding concerns through the Securus monitoring and filtering software. This report is reviewed by the DSL/DDSL and any necessary actions concerned and implemented. An urgent significant (categorised as level 4 and 5 incidents) will be directly emailed to the DSL and Headteacher to ensure they can be dealt with in a timely manner. All actions will be logged on a pupil's safeguarding records and the actions taken recorded in line with the school's Safeguarding and Child Protection policy.

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 /X / 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, newsletters, X 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.

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 Headteacher 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
- The computer in question would be isolated and no changes made to its state.

This policy will be reviewed every year by the Designated Safeguarding Lead (Helen Smith). At every review, the policy will be shared with the Academy Council. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix

1. Responding to an incident Flow chart
2. Acceptable User Agreement - Key Stage 1
3. Acceptable User Agreement - Key Stage 2
4. Acceptable User Agreement – Staff
5. E-safety Incident form
6. E-safety Log

Links

This policy should be used in conjunction with:

- Safeguarding and Child Protection Policy
- Social Media policy
- Staff Code of Conduct
- Positive Relationships and Behaviour Policy
- Anti-Bullying policy
- Victoria Academies Trust GDPR policy
- Disciplinary Policy
- Low Levels Concerns policy

Signed: A-Beaumont

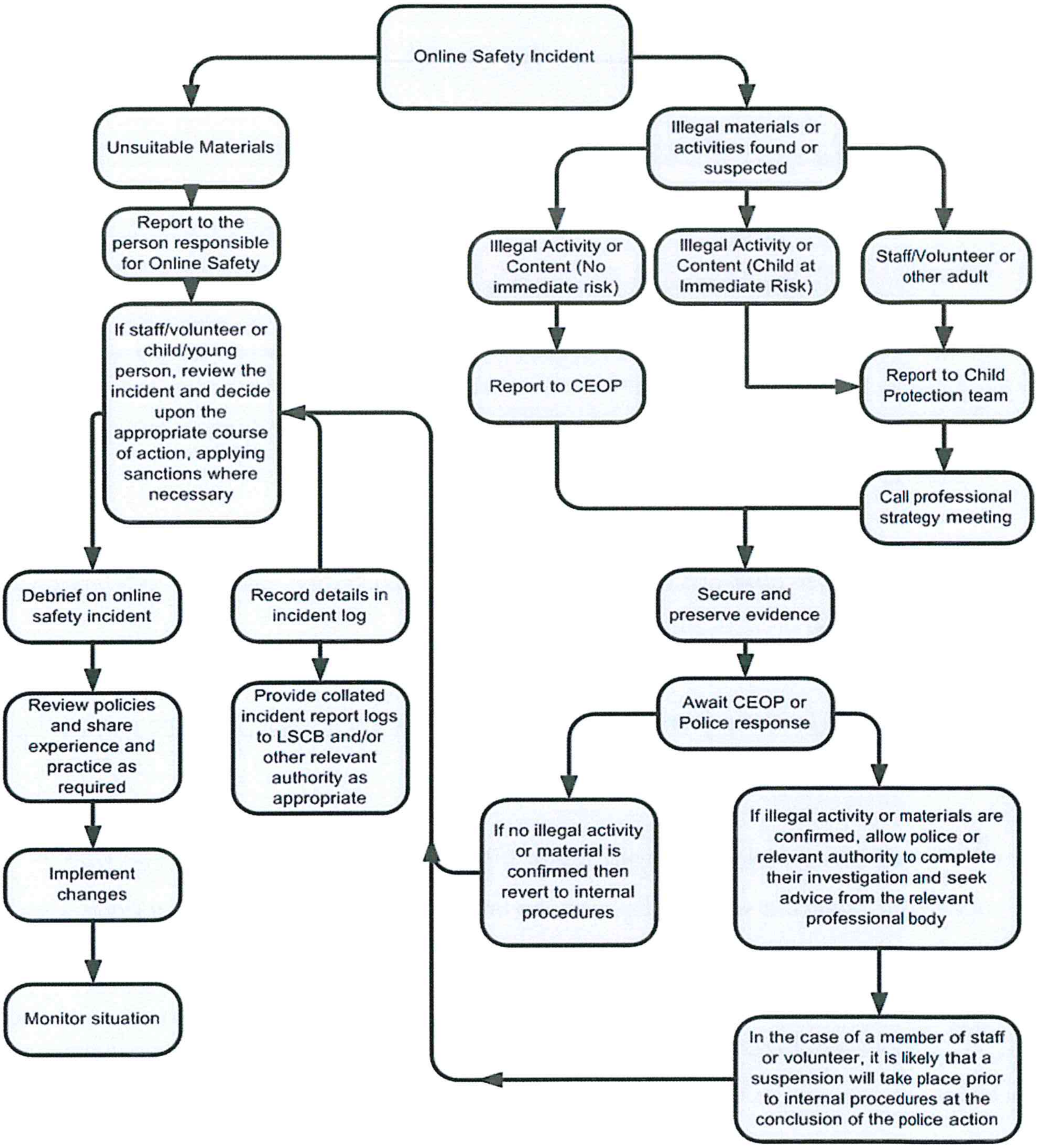
Headteacher

Signed: VMBarr

Chair of Academy Council

To be reviewed: 09-25

Flow Chart – responding to an incident


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

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 can use the internet, computer or ipad

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

S I will look after the computers and ipads and tell the teacher straight away if something is broken or not working properly

S I will only use my passwords and username and not tell them to anyone, including my friends

M I will never give out my personal information (name, address or telephone number) online

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, select a website by mistake or receive a message from anyone I don't know

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

♥ I will be kind to others and not upset them

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 will only use devices and the internet when a teacher/adult is present or with their permission

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

S I will not give my usernames and passwords away and I will tell my teacher if I think someone knows it. I will not use someone else's details and will login off when I've finished.

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.

m I will keep my private information safe and not give my name, address or telephone number to anyone without the permission of my teacher or parents/carers

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

a I will not open any attachments in emails without first checking with an adult

a I will not attempt to download and/or install any unapproved software or resources (including clicking on pop ups) 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.

T I will tell a teacher immediately if I find any material that might upset, distress or harm me, or others.

♡ I will use respectful language when talking to my friends.

♡ I will not make, send or post anything that is likely to upset other children or adults and I will not post/ask them to join a group without their permission.

♡ I will take care of all equipment.

I understand that:

- RPA will monitor my use of ICT in school and on school devices
- I must use school ICT in a responsible way (and for educational purposes) 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 usernames or passwords 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
- I understand that my personal mobile phone must not be out in the classroom/corridors and I cannot talk or send messages whilst I am responsible for children

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 contact ICT tech for advice.
- 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