ROOK’S NEST ACADEMY

COMPUTING AND ESAFETY POLICY 2025

Contents

1 Scope of the Policy 3
2 Roles and Responsibilities 3
Governors: 3
Headteacher and Senior Leaders: 3
Safety Coordinator/Designated Senior Person: 4
ICT Manager (Alamo Support): 4
3 Teaching and Support Staff: 4
Child Protection/Safeguarding Designated Person: 5
Pupils: 5
Parents/Carers: 5
4 Policy Statements 6
Education – students 6
Education – parents/carers: 6
Education – The Wider Community: 7
5 Education & Training – Staff/Volunteers: 7
6 Training – Governors: 7
7 Technical – infrastructure/equipment, filtering and monitoring: 7
8 Use of digital and video images: 8
9 Data Protection: 9
10 Communications: 9
11 Social Media - Protecting Professional Identity: 9
12 Appropriate and Inappropriate Use by Staff or Adults: 10
13 In the Event of Inappropriate Use 10
14 Appropriate and Inappropriate Use by Children or Young People: 10
15 In the Event of Inappropriate Use 11
16 Responding to incidents of misuse: 12

17 Illegal Incidents 12
18 Other Incidents 14
19 APPENDIX 1- Secure transfer of data and access out of Academy 15
20 APPENDIX 2- Staff/Volunteer Acceptable Use Agreement 16
21 APPENDIX 3 – Pupil Acceptable Use Agreement 21

1 Scope of the Policy

This policy applies to all members of Rook's Nest Academy (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Rook's Nest Academy ICT systems, both in and out of Rook's Nest Academy.

The Education and Inspections Act 2006 empowers Headteachers 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 are 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.

Rook's Nest 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 Academy. This policy works together with the academy: Safeguarding, Anti Bullying, Behaviour & Equality Diversity policies.

2 Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Rook's Nest Academy.

Governors:

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

- Regular meetings with the Headteacher
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors

Headteacher and Senior Leaders:

The Headteacher 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 E-safety Coordinator/ ICT Leader.

The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse").

The Headteacher/Senior Leadership Team are responsible for ensuring that the ICT Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in Academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the ICT Manager.

Safety Coordinator/Designated Senior Person:

- leads on e-safety issues
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with relevant bodies
- liaises with Alamo support
- receives reports of e-safety incidents and creates a log of incidents to inform future e- safety developments
- attends relevant meeting/committee of Governors
- reports to Senior Leadership Team

ICT Manager (Alamo Support):

The Network Manager is responsible for ensuring:

- That the Academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the Academy meets required e-safety technical requirements and any Local Authority/other relevant body Computing Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the any networked environments and infrastructure are regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ E-safety Coordinator/Designated Senior Leader for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in Academy policies.

3 Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Academy Computing Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Headteacher/E-safety Coordinator/Designated Senior Person for investigation/action/sanction.
- All digital communications with students/parents/carers should be on a professional level and only carried out using official Academy systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the e-safety and acceptable use agreements.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices. This includes the removal of personal photographic devices that students may bring into the Academy.

- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection/Safeguarding Designated Person:

The Child Protection/Safeguarding Designated Person should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- Should understand the importance of adopting good e-safety practice when using digital technologies out of Academy and realise that the Academy's Computing Policy covers their actions out of Academy, if related to their membership of the Academy.
- Are responsible for using the Academy digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.

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. The Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at Academy events.
- Access to parents' sections of the website and on-line student records.
- their children's personal devices in the Academy (where this is allowed)
- Understand that unacceptable or possibly libelous posts on own social medial accounts, concerning the academy, staff or pupils will be always be challenged

4 Policy Statements

Education – students

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

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

- A planned e-safety curriculum should be provided as part of ICT/PHSE/other lessons and should be regularly revisited. E safety should form part of every computer lesson.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Academy
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents/carers:

Parents/carers play an essential role in the education of their children and in themonitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community:

The Academy will provide opportunities for local community groups/members of the community to gain from the Academy's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e- safety
- The Academy website will provide e-safety information for the wider community

5 Education & Training – Staff/Volunteers:

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy Computing Policy and Acceptable Use Agreements.
- The E-safety Coordinator/Designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Computing Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-safety Coordinator will provide advice/guidance/training to individuals as required.

6 Training – Governors:

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

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- Participation in Academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

7 Technical – infrastructure/equipment, filtering and monitoring:

The Academy will be responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Academy technical systems
- All users will have clearly defined access rights to Academy systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The Academy has provided enhanced/differentiated user-level filtering
- Academy technical staff regularly monitor and record the activity of users on the Academy systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the Academy systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on Academy devices that may be used out of Academy.
- Users are not permitted to download and or install applications (including executable or similar types) on to an Academy device or whilst using the Academy's systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
- CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
- USB Media (memory sticks) – this type of media can be used on Academy devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
- Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

8 Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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:

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents/carers may be given permission 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 students in the digital/video images. If there are children present whose parent/guardian have denied photo permissions then it might be necessary to withdraw permission for any parent to take photos and videos at the event.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes without the permission of the head teacher.

Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of students are published.

Staff must not publish or display photographs or videos of children without ensuring that permission has been granted. A full list of permissions is provided to each teacher.

Student's work can only be published with the permission of the student and parents or carers.

9 Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Academy Data Protection Policy.

10 Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the Academy considers the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- All email messages with the exception of those to and from the Headteacher, SENCO and Business Manager are stored in a central location for 6 months. These emails are accessible by the Headteacher, SLT and ICT Manager.
- Users must immediately report, to the nominated person – in accordance with the Academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, etc.) must be professional in tone and content. Communication between staff and parents should be limited to school hours only 8:30 – 5:00.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Academy/ website and only official email addresses should be used to identify members of staff.

11 Social Media - Protecting Professional Identity:

Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

Academy staff should ensure that:

- No reference should be made in social media to students, 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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The Academy's use of social media for professional purposes will be checked regularly.

12 Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

13 In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

14 Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within Academy, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The children, beginning with years 3 to 6, will study and sign the Acceptable Use Agreement together in class with discussion to ensure a full understanding of the document. Parents will be able to access the document on the school website so that they can see what is expected of their child. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond Academy/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond Academy/education setting or other establishment.

15 In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at Academy, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.

- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

- A record of inappropriate use of technology will be added to the ESafety Incident Log which is maintained by the computing manager.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Use of Mobile Phones and social media (see RNA behaviour policy)

Children are not permitted mobile phones on academy premises.

Many children, especially as they move into KS2 own mobile phones and use social media platforms. This has a potential to lead to problems including bullying and Sexual Violence Sexual Harassment (SVSH) safeguarding concerns (see safeguarding policy). Through PHSE, assemblies and class discussions children will receive instruction on online safety as well as using such platforms respectfully and responsibly.

There are occasions when mobile phones and social media will be used in a negative way by pupils, which can lead to harm and embarrassment to other pupils. Although this often happens out of school hours, the academy will investigate. Parents will be informed and if required external agencies (including the police) will be contacted.

Only those KS2 children who walk home from school and have signed the acceptable use policy may bring a mobile phone. This must be handed in to a staff member before school and returned at the end of the day. Phones must be switched off on school premises.

Children must not use or keep mobile phones on their person whilst in the academy.

Cyber Bullying (see RNA behaviour policy)

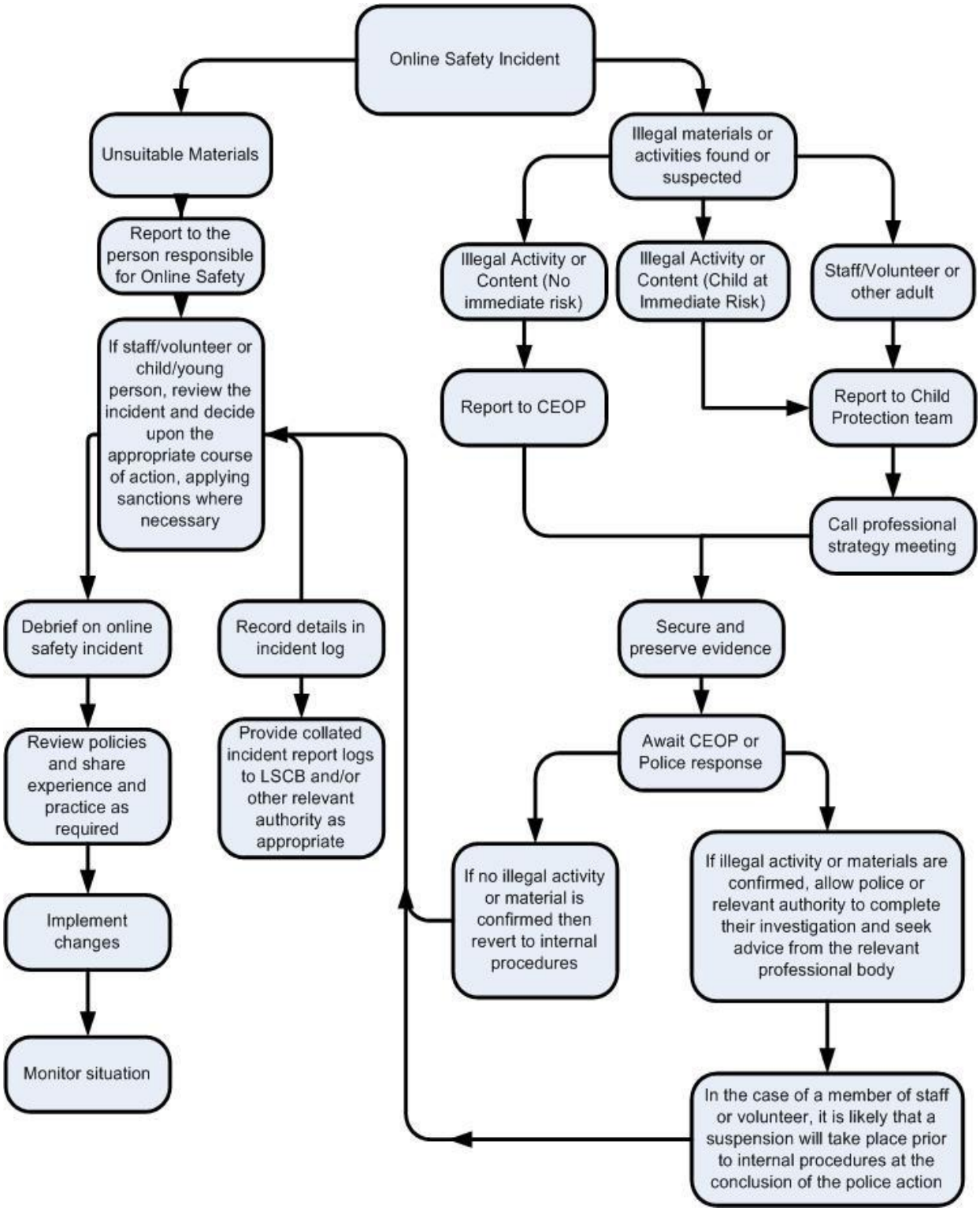
Bullying and abuse through social media is an increasing problem in all areas of society. It is our aim to teach children how to make the right choices of how to deal with and what to do if cyber bullying becomes a problem. PHSE, RHSE & ICT programmes of study cover cyberbullying alongside whole school assemblies. West Yorkshire Police are also proactive in the school regularly delivering assemblies and providing the Academy with POLED (a crime awareness and citizenship scheme of work).

16 Responding to 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 (see "In the Event of Inappropriate Use" above). See flow chart on the next page.

17 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

18 Other Incidents

It is hoped that all members of the Academy community will be responsible users of digital technologies, who understand and follow Academy 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:

1. Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
2. 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.
3. It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
4. 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. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
5. Once this has been completed and fully investigated the group 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:
6. Internal response or discipline procedures.
7. Involvement of a national/local organisation (as relevant).
8. 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' behavior.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- 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.

It is important that all of the above steps are taken as they will provide an evidence trail for the Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

19 APPENDIX 1- Secure transfer of data and access out of Academy

Rook's Nest Academy recognises that personal data may be accessed by users out of the Academy, or transferred to other agencies. In these circumstances:

Users may not remove or copy sensitive or restricted or protected personal data from the Academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of Academy

When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should have secure remote access to the management information system or learning platform

If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

Compliance with the General Data Protection Regulations should be at the core of all data storage, deletion and transfers to and from the Academy.

20 APPENDIX 2- Staff/Volunteer Acceptable Use Agreement

ROOK'S NEST ACADEMY

ACCEPTABLE USE AGREEMENT

(Staff/Volunteer)

2023

New technologies have become integral to the lives of children and young people in today's society, both within the Academy and in their lives outside the Academy. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- Rook's Nest Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

Rook's Nest Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy applies to any device in the Academy. It applies across the whole network and includes Wi-Fi.

Rook's Nest Academy carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Rook's Nest Academy can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by the Academy, logs are kept of activity, whether on an Academy device or using your own device through the Academy Wi-Fi. These logs include who is accessing what material for how long from which device.

The Academy email system is provided for educational purposes, where required the Academy has the ability to access your Academy email for safeguarding purposes.

Acceptable Use Policy Agreement

I understand that I must use Rook's Nest Academy's' ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

I understand that Rook's Nest Academy will monitor my use of the ICT systems, email and other digital communications.

I understand that the rules set out in this agreement also apply to Rook's Nest Academy ICT systems (e.g. laptops, email, etc.) out of Academy, and to the transfer of personal data (digital or paper based) out of Academy.

I understand that Rook's Nest Academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Academy.

I will not disclose my username or password to anyone else, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Rook's Nest Academy ICT systems:

I will not access, 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 not use aggressive or inappropriate language and I appreciate that others may have different opinions.

I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Rook's Nest Academy website) it will not be possible to identify by name, or other personal information, those who are featured.

I will only use chat and social networking sites in Academy in accordance with the Academy's policies

I will only communicate with students and parents/carers using official Academy systems. Any such communication will be professional in tone and manner.

I will not engage in any on-line activity that may compromise my professional responsibilities.

Rook's Nest Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.) in Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

I will not use personal email addresses on the Academy ICT systems.

I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, 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 ensure that my data is regularly backed up, in accordance with relevant Academy policies.

I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this isallowed in Academy policies.

I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.

I will only transport, hold, disclose or share personal information about myself or others as outlined in the Academy Computing Policy, Appendix 3. Where digital personal data is

Transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.

I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Academy sanctioned personal use:

I will ensure that I have permission to use the original work of others in my own work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Rook's Nest Academy:

I understand that this Acceptable Use Agreement applies not only to my work and use of Academy ICT equipment in Academy, but also applies to my use of Academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Academy

I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

ROOK'S NEST ACADEMY

ACCEPTABLE USE AGREEMENT

(Staff/Volunteer) 2023

I have read and understand the above and agree to use the Academy ICT systems (both in and out of Academy) and my own devices (in Academy and when carrying out communications related to the Academy) within these guidelines.

Staff/Volunteer Name

Signed

Date

21 APPENDIX 3 – Pupil Acceptable Use Agreement

Rook's Nest Academy Mobile Phone Contract

Rook's Nest Academy does not permit mobile phones to be brought into school. Phones are expensive items and we cannot guarantee safety or security. This rule is also in place for safeguarding reasons – we cannot filter content to ensure it is appropriate for children if this is accessed on mobile phones. In addition, the taking of photographs etc. needs to be strictly controlled according to parental wishes. Therefore, we ask for your support in NOT sending mobiles into school.

However, we also recognise there may be occasional ***exceptional*** circumstances where it is helpful for a pupil to bring a mobile phone into school, for instance, if they walk to school unaccompanied.

In these circumstances we ask parents and carers to read the following agreement and sign the request, stating the specific reason for a phone to be in school.

Our Pupil Mobile Phone Rules

- All pupils bringing a phone into school must have a good reason for doing so, and must have returned this agreement.
- The school will help children to learn about staying safe online, but recognises that the primary responsibility for online safety at home lies with parents/carers. The school will seek to work with families to help them to encourage children to adopt safe use of mobile technology.
- Children not following these rules will not be allowed to bring a phone into school. **Any phone brought in without permission will be confiscated and only returned to a parent or carer.**
- Children should be reminded not to take photographs or videos of people without asking and never to take them on the way into or out of school or on school premises. **This is because some children are not allowed to have their picture taken.**
- All phones should be turned off before entering school property and must not be turned on until the child is off school property.
- All phones must be handed in to either the staff member on the playground at the start of the day, or to the class teacher on arrival in class.
- The school cannot accept responsibility for damage or loss of a mobile phone brought into school.
- The school has the right to confiscate or search a mobile phone. In the unlikely event of needing this, we will endeavour to contact a parent or carer. As part of this agreement, your child should agree to unlock the phone if required by a member of staff. If a phone has been confiscated it will be for not following this contract and will only be issued back into the care of an adult.
- In the event of a child using a phone in an unsafe way, causing potential harm to themselves or another child, even outside of school hours, the school may refuse permission for that child to bring a phone into school under any circumstances.
- We currently advise that the use of Smart Watches is prohibited in school.

Parents may want to look at the advice on www.internetmatters.org which explains how to add some parental controls to the phone and gives advice on how to keep children safe.

Please sign and return the agreement overleaf.

Rook's Nest Academy

Mobile Phone Agreement
Our Pupil Mobile Phone Rules

- All pupils bringing a phone into school must have a good reason for doing so, and must have returned this agreement.
- The school will help children to learn about staying safe online, but recognises that the primary responsibility for online safety at home lies with parents/carers. The school will seek to work with families to help them to encourage children to adopt safe use of mobile technology.
- Children not following these rules will not be allowed to bring a phone into school.
- Children should be reminded not to take photographs or videos of people without asking and never to take them on the way into or out of school or on school premises.
- All phones should be turned off before entering school property and must not be turned on until the child is off school property.
- All phones must be handed in to either the staff member on the playground at the start of the day, or to the class teacher on arrival in class.
- The school cannot accept responsibility for damage or loss of a mobile phone brought into school.
- The school has the right to confiscate or search a mobile phone. In the unlikely event of needing this, we will endeavour to contact a parent or carer. As part of this agreement, your child should agree to unlock the phone if required by a member of staff. If a phone has been confiscated it will be for not following this contract and will only be issued back into the care of an adult.
- In the event of a child using a phone in an unsafe way, causing potential harm to themselves or another child, even outside of school hours, the school may refuse permission for that child to bring a phone into school under any circumstances.
- We currently advise that the use of Smart Watches is prohibited in school.

Name of Child:

_____

Reason for needing a mobile phone in school:

_____

_____

_____

Parent/Carer: I confirm that I have explained the school rules regarding mobile phones to my child and confirm that they may take a mobile phone into school on that basis.
Parent/Carer signature _____ Date _____
Pupil: I will follow the school mobile phone rules.
Pupil signature _____ Date _____

After consideration of the reasons stated for your child to bring a mobile phone into school the Academy accept/decline your request.
Permission for a mobile phone is granted/not granted

Signed on behave of RNA:
Date: