18 37

Roundhay St. John's

Online Safety Policy

Approved by:	Pupil Support Committee
Date:	July 2021, Updated July 2022
Next review due by:	Full review July 2024

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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
- 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.

The policy also takes into account the National Curriculum computing programmes of study

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will ensure there appropriate discussion about online safety through the Pupil Support Committee who will receive regular reports from the Online Safety Lead and the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Headteacher

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

3.3 The Online Safety Lead

Mrs Richards, the online safety lead, 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, ICT Manager (Datacable), Business Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) 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 behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and the Pupil Support Committee of the governing board
- Providing day to day guidance for school-based staff

3.4 The ICT Manager (Datacable)

The ICT manager, with the support of the School Business Manager, is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- The Business Manager will ensure that any online safety incidents are passed to the classteacher and Online Safety Lead who will ensure that they are followed up and logged (see appendix 5) appropriately in line with this policy

3.5 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the online safety lead to ensure that any online safety incidents are logged (see appendix 5) 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 behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents 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 (appendices 1 and 2)

Parents 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 International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 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 acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, 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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the online safety lead.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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 online safety lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers (where appropriate) and governors are expected to agree and abide by the school's acceptable use policy regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils will not bring any mobile devices to school unless express permission has been granted by the headteacher. Any use of mobile devices in school by pupils and agreed by the headteacher must be in line with the acceptable use agreement (see appendices 1 and 2).

Where any pupils do bring a mobile device into school for safeguarding purposes for their journey to and from school, these must be taken to the school office on arrival and collected on departure.

Any breach of the acceptable use agreement by a pupil will be dealt with in line with the school behaviour policy.

9. Remote access

We allow staff to access the school network remotely. Remote access is coordinated by Datacable and teaching staff receive instructions on how they get such access. Only school devices are permitted to be used to access the school server remotely.

Staff accessing the school's network remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use school's ICT facilities outside the school and take such precautions as the headteacher, SBM, ICT manager (Datacable) or Online Safety Lead require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

10. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practises at all times.

10.1 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any person using personal devices to use the school's Wi-Fi must log in as a guest. All staff and visitors are expected to turn off their mobile data whilst in school and revert to the school's Wi-Fi network.

10.2 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

11. Training

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).

The DSL and deputies 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety as outlined in section 3. An incident report log can be found in appendix 5.

This policy will be reviewed annually by the Pupil Support Committee in conjunction with the headteacher and the online safety lead. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

This is how I stay safe when I use computers and computing equipment:

- Ask a teacher or adult if I can do so before using them
- Only use websites, devices, apps or games that a teacher or adult has told me or allowed me to use
- Only use the computer equipment or internet **when an adult is with me**
- Tell my teacher or trusted adult immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the usernames and passwords I have been given to log in and try my hardest to remember them
- Never share my password with anyone, including my friends
- Never give my personal information or other peoples' personal information (name, address, telephone numbers or photograph) to anyone without the permission of my teacher or parent/carer
- I will not take photographs or recordings of myself or other people unless my teacher has told me I can
- Save my work on the school network
- I will not bring any ICT equipment in from home (including: mobile phone, memory stick, ipad, camera)

I agree that the school will monitor the websites I visit, the work I complete and the things I save and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement:

Parents are asked to support the school's agenda in relation to online safety and the observance of this policy and also:

- To acknowledge that the school may pass on my child's personal data (such as name, age and school year) to third party on-line providers of educational activities (such as Tapestry, Purple Mash, Times Tables Rockstar). To consent to this to the extent necessary for my child to take part in such activities;
- To keep any school usernames and passwords secure and to respect any technical safeguards in place;
- To acknowledge that the manner in which my child uses school platforms in the home environment and the monitoring of this is my responsibility;
- To generally observe good 'netiquette', including being considerate when communicating with the school, for example, appreciating that any messages sent to school will only be responded to within school hours and within a reasonable time period, and being courteous when communicating with the school;
- To consider carefully the impact of any comment made on social media about the school / school community or member of staff before posting;
- To refrain from posting any personal information / photos about any child / parent / teacher (or other person connected to the school) on social media without their consent;
- To acknowledge that the filtering systems at home are different to those the school has in place and that when using technology at home, these become the responsibility of the parents / carers.

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for school work only
- Make sure the messages I send or the information I upload, is polite, truthful and sensible
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address, telephone number or photograph to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it
- Understand that some social networking sites, apps and games have an age restriction and I will honour these and only access the ones I am old enough for and my teacher has given me permission to access

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Share my address, phone number, upload a picture / recording or give any other personal information that could identify myself, my family or any other person
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details or alter anyone else's work
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Bring any personal device in from home unless I have been given permission from the headteacher

I agree that the school will monitor the websites I visit, the work I complete and the things I save and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement:

Parents are asked to support the school's agenda in relation to online safety and the observance of this policy and also:

- To acknowledge that the school may pass on my child's personal data (such as name, age and school year) to third party on-line providers of educational activities (such as Tapestry, Purple Mash, Times Tables Rockstar). To consent to this to the extent necessary for my child to take part in such activities;
- To keep any school usernames and passwords secure and to respect any technical safeguards in place;
- To acknowledge that the manner in which my child uses school platforms in the home environment and the monitoring of this is my responsibility;
- To generally observe good 'netiquette', including being considerate when communicating with the school, for example, appreciating that any messages sent to school will only be responded to within school hours and within a reasonable time period, and being courteous when communicating with the school;
- To consider carefully the impact of any comment made on social media about the school / school community or member of staff before posting;
- To refrain from posting any personal information / photos about any child / parent / teacher (or other person connected to the school) on social media without their consent;
- To acknowledge that the filtering systems at home are different to those the school has in place and that when using technology at home, these become the responsibility of the parents / carers.

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Staff acceptable use agreement

Roundhay St John's CE Primary Acceptable Policy

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.
- that school 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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 school.
- 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 Online Safety Leader or the Headteacher.

I will be professional in my communications and actions when using school 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 school'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 (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking sites for personal use in school. These sites may be used in direct relation to requirements for Teaching and Learning or other activities directly related to the work of the school e.g. PTA Facebook page / Oakwood Church.
- I will only communicate with pupils and parents / carers using official school 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.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school 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 school 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 school 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. I will request these changes be made by the school's technician.
- I will not disable or cause any damage to school 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 School Personal Data Policy (or other relevant policy). 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 pupil 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 school 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 school sanctioned personal use:

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

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.
- I understand that I am required to leave my mobile device in a safe place during the school day and only use this in areas of the school that the pupils are not permitted. By signing this agreement, I am agreeing to turn off my mobile data and switch my mobile device to the school WIFI as a guest.

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

Staff / Volunteer Name: ....

Signed: ....

Date: ....

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

Roundhay St John’s CE Primary School

Record of Online Safety Incidents

All completed forms will be given to the Headteacher who will store them in the ‘Online Safety Incident File’ in the office.

Name of person / people involved:	Date

Reason for investigation Please specify the device the incident occurred on, the address of any websites and the main reason for concern.

First reviewing person

Name	Position	Signature

Second reviewing person

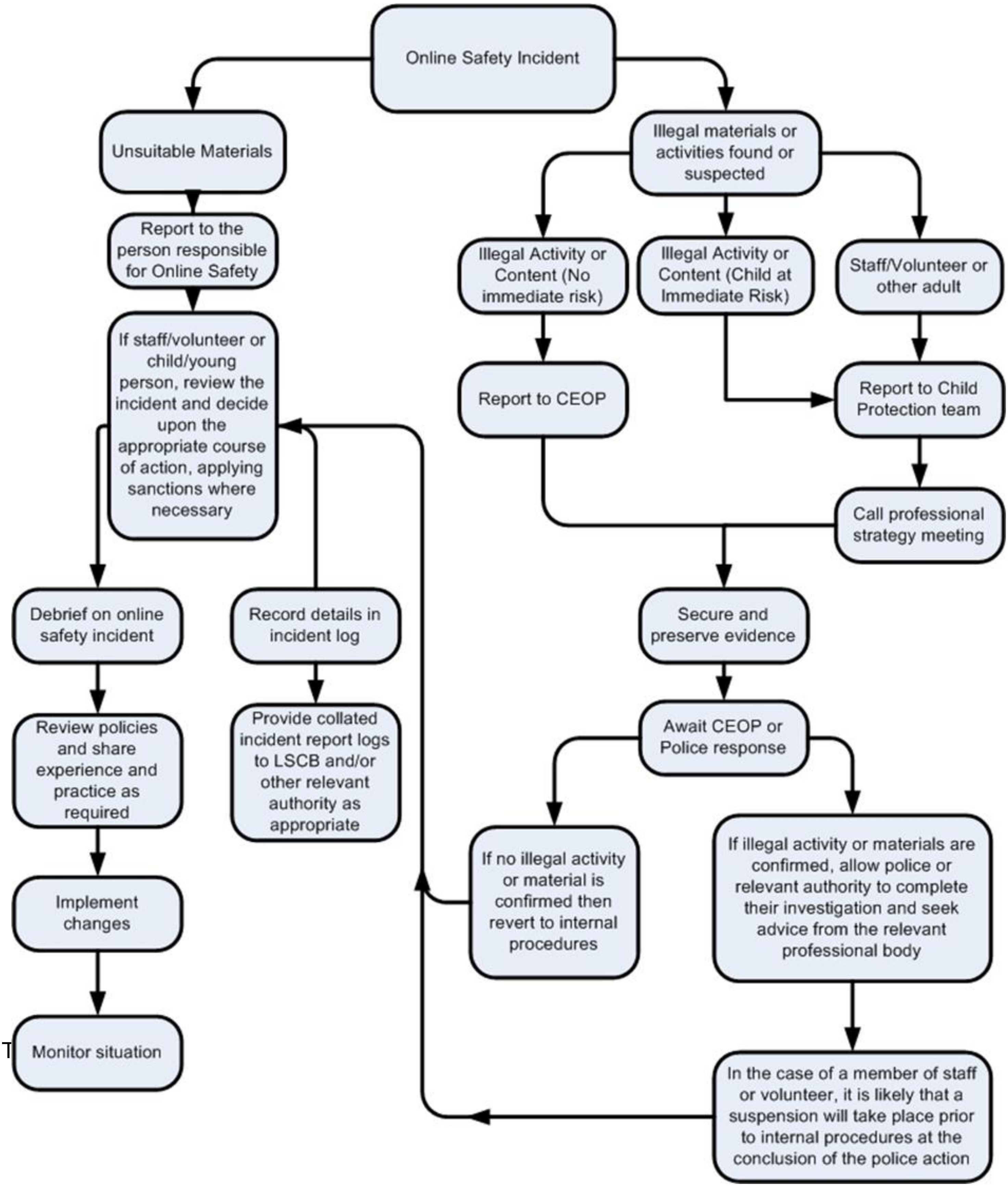
Name	Position	Signature

Conclusion and proposed actions to be taken

Appendix 6: Online Incident Flow Chart

Roundhay St John’s CE Primary School

Online Incident Flow Chart


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

T