Roundhay St John's CE Primary School

Online Safety Policy

Headteacher:	L Briggs
Chair of LAC:	J Thompson
Date:	March 2026
Next review due by:	March 2027

Contents

1. Introduction and Aims

Information communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

Our school aims to:

- Have robust guidelines, rules and processes in place to ensure the appropriate use of school ICT resources and the online safety of pupils, staff, volunteers and governors
- Identify and support groups of children that are potentially at greater risk of harm online than others
- Prevent disruption that could occur to the school through misuse, or attempted misuse, of ICT systems
- 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 phones and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremeism
- **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 the user 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

This policy covers all users of our school's ICT facilities, including pupils, staff, governors, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Handbook and School Behaviour Policy.

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
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

This policy 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.

In addition to the above, this policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications Regulations 2000
- Freedom of Information Act 2000
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes: advice for educational settings working with children and young people
- Meeting digital and technology standards in schools and collages

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

3. Roles and responsibilities

3.1 The Local Academy Council (LAC)

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

The LAC will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The LAC will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The LAC will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The LAC will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The LAC will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is Gemma Fleury (safeguarding governor)

All governors will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher and Designated Safeguarding Lead (DSL)

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

Details of the school's designated safeguarding lead (DSL) and deputy DSLs are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and make sure 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT 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
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure 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/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils 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.

3.3 The Online Safety Lead DSL responsibilities

The online safety lead is the DSL/headteacher and 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 (Primary ICT), 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 LAC

- Providing day to day guidance for school-based staff

3.4 The ICT Manager (Primary ICT)

The ICT manager, with the support of the School Business 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 make sure 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 through Securly, the school's monitoring and filtering system, 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 DSL/Online safety lead/headteacher is provided with a monthly Securly report and will ensure that any online safety incidents are followed up and logged (see appendix 5) appropriately in line with this policy *
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure 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.

3.5 All staff, governors, visitors and volunteers

All staff, including contractors and agency staff, governors, visitors 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 (as outlined in appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 contacting Primary ICT Support through submitting a ticket or notifying the DSL/Online safety lead/ headteacher.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes by contacting Primary ICT Support through submitting a ticket or notifying the DSL/Online safety lead/ headteacher.
- Working with the DSL 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
- 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'

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
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

Access to ICT facilities and materials

Parents and carers do not have access to the school's ICT facilities as a matter of course. However, parents / carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or permitted to use the school's facilities at the headteacher's discretion by using a time-limited visitor login.

Where parents / carers are granted access in this way, they must abide by this policy as it applies to staff and agree to follow the 'Staff, Governor, Volunteer and Visitor Acceptable Use Agreement (appendix 3).

Communicating with or about the school online

We believe that it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents / carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through the website or social media channels.

We ask parents / carers to sign the agreement in appendix 1 / 2

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

4.1 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
- Be discerning in evaluating digital content

*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*

From September 2026

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

At Roundhay St John's we use 'Project Evolve' as the basis for our teaching of online safety. We have used their resources to create a whole school long term plan covering Nursery through to Year 6.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

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. This policy will also be shared with parents / carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher (DSL) and/or Deputy Safeguarding Leads

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. Teachers will discuss cyber-bullying with their classes.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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 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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in our school's behaviour policy), 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 for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL.
- Explain to the pupil why they are being searched, and 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 the staff member in conjunction with the DSL / 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 whether 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
- Our behaviour policy

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

6.4 Artificial intelligence (AI)

Generative 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 Gemini.

Roundhay St John's recognises that AI has many 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.

Roundhay St John's will treat any use of AI to bully pupils very seriously, in line with our behaviour policy policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy. The Responsible Use of Artificial Intelligence (AI) in School Policy must be read and signed off prior to any AI usage in school.

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 to ensure they comply with the above and in order to:

Safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network.

This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and Primary ICT, as appropriate.

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, including wearable tech, unless express permission has been granted by the headteacher and parents have agreed to abide by the school's acceptable use agreement. 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 and use of work devices outside school

We allow staff to access the school's ICT facilities and materials remotely. Remote access is coordinated by Primary ICT 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 should dial in using a virtual private network (VPN).

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Headteacher, SBM, ICT manager (Primary ICT) or Online Safety Lead require 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, which can be found in the staff handbook.

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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- 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
- Keeping operating systems up to date by promptly 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 3.

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 the DSL/online safety lead or Primary ICT Support.

10. 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 behaviour and ICT and internet acceptable use . 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 disciplinary procedures. 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.

10. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in

place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber-crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

10.1. Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager required by the ICT service providers to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

10.2 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 have these installed, and 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 personal devices using the school's network must all be configured in this way.

10.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy, which can be found in the Staff Handbook.

10.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher or member of the central team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

10.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT service provider.

11. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology. The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - Proportionate: the school will verify this using a third-party audit annually, to objectively test that what it has in place is effective
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    - Up to date: with a system in place to monitor when the school needs to update its software
    - Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be
- Back up critical data at least once a day and store these backups on cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT provider.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
-

12. Training for staff, governors and volunteers

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, Bitesize training (Clennell) 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 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.

Governors 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.

13. 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 headteacher / DSL/ Online safety lead in conjunction with the headteacher and the online safety lead. At every review, the policy will be shared with the LAC. The review will be supported by an annual risk assessment (produced by SWGfL) 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.

14. 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
- Computing Policy
- Acceptable Use Policy
- Responsible Use of Artificial Intelligence (AI) in Schools Policy
- Staff Handbook

- Finance Policy
- Scheme of Delegation

Appendix 1: EYFS, KS1 and Parent / Carer Acceptable Use Agreement

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
- Check with my teacher before I print anything
- Log off or shut down a computer or other device when I have finished using it
- I will not bring any ICT equipment in from home (including: mobile phone, wearable tech, 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: 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 will make sure my child understands these.

In addition to supporting the above, ***parents / carers*** *are asked to* ***read and sign*** *the* ***parent / carer agreement*** *on the* ***back of this sheet.***

Signed (parent / carer):	**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;

Online channels are an important way for parents / carers to communicate with, or about, our school. The school uses the following channels: Our o*fficial Facebook page*; *Email / text groups* for school announcements; our *virtual learning platform.*

Parents / carers also set up independent channels to help them stay on top of what is happening in their child's class. For example email groups or chats through apps such as WhatsApp.

When communicating with the school via official communication channels or using private / independent channels to talk about the school, I will:

- Observe good 'netiquette', including being considerate and respectful when communicating with the school / staff;
- Be respectful of other parents / carers and children;
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure;
- Appreciating that any messages sent to school will only be responded to within school hours and within a reasonable time period;
- 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 will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff;
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I am aware of a specific behaviour issue or incident;
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of all of the other children's 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. I agree to abide by the Parent / Carer Acceptable Use Agreement outlined above.

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

If I have been given permission to bring a personal mobile phone or other electronics device into school, including wearable tech:

- I will hand it in to be stored securely by my teacher
- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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's agreement: 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.

In addition to supporting the above, ***parents / carers*** *are asked to* ***read and sign*** *the* ***parent / carer agreement*** *on the* ***back of this sheet.***

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (parent / carer):	**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;

Online channels are an important way for parents / carers to communicate with, or about, our school. The school uses the following channels: Our o*fficial Facebook page*; *Email / text groups* for school announcements; our *virtual learning platform.*

Parents / carers also set up independent channels to help them stay on top of what is happening in their child's class. For example email groups or chats through apps such as WhatsApp.

When communicating with the school via official communication channels or using private / independent channels to talk about the school, I will:

- Observe good 'netiquette', including being considerate and respectful when communicating with the school / staff;
- Be respectful of other parents / carers and children;
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure;
- Appreciating that any messages sent to school will only be responded to within school hours and within a reasonable time period;
- 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 will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff;
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I am aware of a specific behaviour issue or incident;
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of all of the other children's 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. I agree to abide by the Parent / Carer Acceptable Use Agreement outlined above.

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

Appendix 3: Staff, Governors and Visitor acceptable use agreement

Roundhay St John's CE Primary Acceptable Policy

The school's Headteacher manages access to the school's ICT facilities and materials for school staff, governors and visitors with the support of the Primary ICT technician and the School Business Manager. That includes, but is not limited to:

- Computers, mobiles phones and other devices
- Access permissions for certain programmes or files

Staff, governors and visitors will be provided with unique login / account information and passwords that they must use when accessing the school's ICT facilities. Staff must speak to the Headteacher / School Business Manager to request these.

Staff , governors and visitors who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Headteacher, who will instruct Primary ICT.

This Acceptable Use Policy is intended to ensure:

- that staff, governors 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 all users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff, governors and visitors are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff, governors 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; to safeguard and promote the welfare of children and provide them with a safe environment to learn:

- I understand that the school will filter and monitor my use of the school ICT facilities and network including digital technology and communications systems as outlined in the Monitoring section of the Online Safety Policy
- I understand that the rules set out in this agreement also apply to use of the school ICT facilities and network (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 professional use.
- I understand that use of the school's ICT facilities and network, for personal use may put personal communications within the scope of the school's ICT monitoring activities (see Monitoring section). Where breaches of this policy are found, disciplinary action may be taken.
- I will login to the school's ICT facilities and network using the username and password I have been assigned.
- 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 DSL or the Headteacher.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will be professional in my communications and actions when using school ICT systems:

- I will use my work email account for work purposes only. All work-related business will be conducted using the email address provided by the school.
- I will enable multi-factor authentication for my email account.
- 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.
- I will ensure my use of all forms of social media, either for work or personal purposes, is appropriate at all times.
- 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 or for any school business.
- 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.
- I will ensure I encrypt any sensitive or confidential information so that the information is only accessible by the intended recipient.
- I will inform the Data Protection Officer, Leanne Noone, immediately and follow the school's data breach procedure if I send an email in error that contains the personal information of another person.
- If I receive an email in error, I will inform the sender and delete the email immediately. The information contained within the email will remain confidential.

When using the school's ICT facilities / 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 personal use of the school ICT facilities is permitted occasionally provided that such use does not take place during contact time / teaching hours / non-break time; does not constitute 'unacceptable use'; takes place when no pupils are present; does not interfere with my work, prevent other staff / children from using the facilities for work or educational purposes.

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