Online Safety Policy

St Peter and St Paul CE Academy - Rise Multi-Academy Trust

September 2024

Review Date: September 2026

Introduction

This Online Safety policy recognises the commitment of St Peter and St Paul CE Academy to keeping staff and pupils safe online and acknowledges its part in the Trust's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe that the school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm (DfE Keeping Children Safe in Education 2016)

Our academy is committed to developing a set of safe and responsible behaviours that will enable all stakeholders to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary, disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the network and facilities from attack, compromise and inappropriate use and to protect Trust and school data and other information assets from loss or inappropriate use.

The impact of the Covid-19 pandemic and the requirement placed upon schools to deliver remote learning has further raised the profile of the importance of online safety. **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 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 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.

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

Roles and Responsibilities

Governors

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and any online safety incidents logged on CPOMs as provided by one of the designated safeguarding leads (DSLs).

The governor who oversees online safety is _____*check who it is*.

All governors will:

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

The headteacher

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

Designated Safeguarding Leads

Our DSLs take 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 and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs 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 behaviour policy
- Liaising with other agencies and/or external services if necessary This list is not intended to be exhaustive.

The ICT technician

The ICT technician (employed by ICTtechie) 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
- Ensuring that any online safety incidents are logged, shared with a DSL 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.

ICT curriculum coordinator

The coordinator for the teaching of computing will ensure that:

- They are able to liaise with the technician on aspects listed above.
- Opportunities to teach online safety appear in our curriculum offer (also facilitated by the PSHE coordinator and curriculum coordinator).
- Staff training opportunities are planned addressing how staff can keep themselves and pupils safe online – particularly, when remote learning, MS Teams lessons etc are necessary.

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 and ensuring that pupils follow the school's terms on acceptable use (appendix 3)
- Working with the Head teacher and DSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

  (This list is not intended to be exhaustive).

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 (appendix 3)

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

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).

Educating pupils about online safety

Pupils are taught about online safety as part of the curriculum:

The introduction of the new relationships education and health education curriculum is compulsory from September 2021 but our academy have begun to roll it out from the start of 2020/21 to ensure aspects such as online safety are as prominent as possible. We have selected a range of learning opportunities from the PSHE association planning tool that are appropriate for the needs of our pupils and have ensured that the outcomes listed in the 'by the end of Primary School' section are covered.

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
- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help.

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.

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

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

Any devices loaned to parents/children in instances of remote learning being necessary will contain information to be signed relating to acceptable use and online safety.

Use of the internet to carry out virtual lessons on MS Teams

This has been necessary during instances of isolation linked to Covid 19 and throughout the pandemic in general. Parents have been notified of expectations of conduct within these sessions and this detail is also outlined in our remote learning policy. It will be necessary to reissue these guidelines as a reminder, in future, should further isolations take place.

In order that safeguarding risks are not posed, parents are asked to support their child in ensuring that:

- they don't carry out lessons alone in their bedrooms
- they are mindful of their own conduct and what can appear in the background
- they turn their cameras off if a child is not permitted to appear online
- they mute themselves unless they are asking or answering questions or have been directed to unmute by the teacher.

Teachers ensure safeguarding is not compromised by:

- ensuring that recordings of sessions are only available in their own chat function and not in those of the children.
- When they make recordings available to children, this is done via MS Streams so that it cannot be downloaded or altered by children

- They regularly remind children of protocols above
- They are mindful of their own surroundings, especially when working from home
- They have another adult such as a Learning Support Assistant online with them during any sessions with groups or individual pupils.

Further detail of online safety relating to remote learning can be found in the Rise Remote Learning Protocol (appendix 1) and the remote learning policy.

Loaning internet ready devices to pupils/families

In this instance, parents must sign the loan agreement (appendix 2) to agree that the device will not be used inappropriately. This is talked through with parents and pupils upon receipt of the device.

Cyber-bullying

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.

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 such as in PSHE as previously described.

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

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 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.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or •

  Report it to the police

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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..

Pupils using mobile devices in school

Some pupils in upper Key Stage 2 bring mobile phones to school for safety purposes when walking home independently. In these instances, they should be handed in to the school office or class teacher on arrival, to be collected at home time. They should not be used within school hours or left in bags throughout the day.

Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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 (facilitated by the ICT technician)
- Keeping operating systems up to date – installing the latest updates

Staff members must not use the device in any way which 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 a member of ICT techie or, where relevant, Primary World who support us with use of Outlook, MS Teams etc.

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 acceptable terms of use of the internet. 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 policy on 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

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

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

The DSLs 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMs

This policy will be reviewed every three years by the deputy head teacher. At every review, the policy will be shared with the governing board.

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
- Remote learning policy

Appendix 1 – Rise online learning protocols

Rise Remote Learning Protocol

St Peter & St Paul CE Academy, February 2021

This protocol applies to all schools in the Rise family.

Parents/carers are responsible for ensuring that during the session children:

- understand that a Teams session will be subject to the same school rules which apply in face-to-face lessons
- will follow all instructions issued by their teacher, only using technology as they direct them to do
- will join the Teams session 5 minutes before it begins and join a waiting room until the time the session is due to start
- will make sure their communication with teachers and other pupils is appropriate of a normal classroom environment
- will be responsible for their behaviour and actions when using Teams or any other online platform
- will not deliberately access or share any material which could be deemed illegal or offensive. If they come across such material, they will report it to a suitable adult, either the teacher or parents
- understand that a member of the Senior Leadership Team may attend any Teams session
- will not record or take photos of teachers or pupils, or any lesson content
- understand that these rules are designed to keep their children safe and that, if they are not followed, the normal school Behaviour Policy will be invoked
- will ensure that pupils are suitably dressed and are supported by an adult
- when possible will facilitate the session, even if they are undertaking other tasks or monitoring other children
- If there is a serious breach of conduct, teachers will remove the person immediately. If this should happen, an email/phone call will be sent/made to confirm the reasons why

Parents should respect the classroom environment and not become involved in the ongoing live lessons, unless invited to do so by the teacher.

Report any concerns as soon as possible.

No parent or pupil shall make any photo/screenshot, video or audio recording of any of the online teaching or live lessons.

If a teacher or member of school staff believes that this is happening, that pupil or parent will be ejected from the session. This will be a breach of the school behaviour/discipline policy.

The school may take reasonable measures to be certain that any such recording shall be deleted.

Remote Learning for children

- Ensure you are in a quiet, safe and appropriate environment with minimal distractions. A bedroom is not a suitable location; a dining or kitchen table, if suitably quiet, may be appropriate.
- Log in 5 minutes before your session.
- Dress appropriately. You may not wear nightwear.
- Ensure you are attentive and follow all instructions, treating others with kindness and patience, particularly where technical issues cause disruption and being respectful at all times, e.g. taking turns, not eating or drinking during the session, not getting up to do other things.
- End your session when your teacher indicates it is complete.
- You may not record lessons or any other online interactions.

When you join a remote learning session we expect that you are agreeing to meet these expectations for learning.

The school shall have the benefit of the copyright for all material supplied. There is no consent for any material to be shared on social media or on the internet without the express written consent of a member of the school Senior Leadership Team. These rights will be actively pursued.

The Remote Learning Protocol is to work in conjunction with the schools Safeguarding and Promoting the Welfare of Pupils Policy, Anti-Bullying Policy and the Internet and E-Safety Policy.

Appendix 2 –

Loan agreement for devices issued to families during periods where remote learning is necessary.

- I will ensure that my child's laptop is kept in its protective case at all times.
- I will ensure that my child doesn't share the passcode or device with anyone else in my household.
- I will ensure that my child uses the laptop for school work and homework only.
- I will ensure that my child will not behave in a way that can cause damage to the laptop.
- I will ensure that my child will not give my home address or telephone number, or arrange to meet someone and adhere to all e-safety guidance.

- I will ensure that my child will bring the laptop to school when they return.
- I understand that the school will monitor the laptops and have the rights to install/remove apps, change the laptop settings, check the files and may monitor the Internet sites I visit.
- I understand that use of the laptop is subject to the schools Acceptable Use of

ICT Policy

- By signing this form, I am agreeing to the terms above on the loan of the laptop

  for my child.

Appendix 3

Pupil's acceptable use agreement

RULES FOR INTERNET SAFETY

As part of the ICT curriculum, your child will be taught to use the Internet and other digital technologies to search for information which helps to promote creativity and provides a more exciting and challenging classroom experience. We aim to teach all pupils skills of critical awareness, digital literacy and good online citizenship to enable them to use the internet and other digital technologies safely both at school and at home. We have taken a range of measures to minimise risks associated with using the internet at school. These include:

- Operating a high level filtering system.
- Supervision by an adult to access the internet.

- Not allowing access to chat rooms at any time other than discussion forums approved and explained by a member of staff.
- Teaching children about safe internet.

In order to ensure that children are able to use the internet safely, parents must first complete and return the school copy of this agreement to confirm they have understood and shared the following rules with their child.

1. **I will always ask an adult when I use the internet and will be sensible whenever I use it.**
2. **I will only use the internet for schoolwork and homework and will only use sites an adult has told me about.**
3. **I will not give my name, address, telephone number or date of birth to anyone on the internet and will tell an adult if anyone asks me for any personal information.**
4. **I will never agree to meet anyone I have communicated with on the internet.**
5. **I will always use acceptable words in emails, communicating via text messages and when using discussion forums.**
6. **If I see anything I am unhappy with or I receive a message I do not like, I will tell an adult immediately.**
7. **I will not share any passwords.**

I have read and understood the school rules for online safety and have discussed them with my child. I give permission for my child to use the school's computing systems including the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I will not take pictures or video my child on school premises and upload onto social media.

Signed_____

Parent/Person with legal responsibility for the child

Date_____

Staff acceptable use agreement (I couldn't find one from our school so have inserted the Key's one here).

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first

- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the school.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed _____