Rainford High

Online Safety Policy

Everyone Matters

We expect our community to be kind, polite and respectful

Everyone Helps

We expect our community to make sensible choices

Everyone Succeeds

We expect our community to work hard

Guidance Owner	Principal
Policy responsibility	Safeguarding Lead
Scope of the Policy	Rainford Academies Trust
Written/last reviewed	**June 2023**
Next review due	**June 2024**
Summary of key changes	Added further information on monitoring and filtering and online safety. Added support list for parents/carers.

Contents

---

1. Aims

Our school aims to:

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

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for principals and school staff
- [Relationships and sex education
- Searching, screening and confiscation
- The Prevent Duty – Department Advice for Schools and Childcare providers

It also refers to the Department'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.

3. Roles and responsibilities

3.1 The trustee board

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

The trustee board will review this policy regularly as part of safeguarding reviews with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The trustee who oversees online safety is Jayne Lloyd.

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet – see the acceptable use policy.

3.2 The principal

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

3.3 The designated safeguarding lead

Details of the school's DSL, Deputy DSL and DS Officers are set out on our school website under safeguarding.

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

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the principal and/or trustee board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems constantly, including network monitoring, office 365 account monitoring, anti-virus software. There are also security audits being carried out.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the principal 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

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

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.

4. Educating pupils about online safety

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

From September 2020 **all** schools will have to teach:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Online safety is also covered in ICT lesson and PSHE, along with parents receiving supporting materials from our subscription to the National Online Safety website. We have now received recognition for our commitment to improving online safety at Rainford.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, in information via our website and through encouraging engagement in the National Online Safety subscription. 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 principal and/or the DSL.

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

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 and the anti-bullying 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. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. This will be carried out in line with our peer to peer allegations policy appropriate.

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.

6.3 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and trustees 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, trustees and visitors to ensure they comply with the above. We also use secures software to monitor use of the computers.

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

Lessons

Tutor group time

Clubs before or after school, or any other activities organised by the school

During break or lunchtime

We operate the policy of: Hear it, see it, use it, lose it, unless authorised to do by a member of staff.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. We strongly discourage any use of USB devices.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

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 in our behaviour for learning, safeguarding and exclusions policies. 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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 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.

Trustees 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.

12. Monitoring arrangements

The DSL, Deputies and officers along with the pastoral team log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the trustee board.

13. Prevent Duty

We have the Prevent duty to adhere to in our school. We have our filtering and monitoring systems, namely London Learning Grid and Securus, to identify concerns in relation to prevent. This is reported to the school Designated Safeguarding Lead and Prevent Lead.

Prevent education is provided through the online safety curriculum to support students keeping safe online. This is embedded on our RSE/PSHE curriculum.

Staff are provided with training about the harms of online activity of extremist and terrorist groups.

14. Online Safety

We are aware of the online safety risks that our pupils face and the increased risks since post lock down. It is essential that children are safeguarded from potentially harmful and inappropriate online conduct, content, contact and commerce.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, 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
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your child is at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

At Rainford we have our online safety policy and we review our online safety provision annually through an audit to ensure that our curriculum and measures in place are suitable and relevant in supporting the safeguarding our pupils.

Staff are provided annual online safety training so they are aware of the risks online, what to watch out for and they are trained in what to do if they have a concern, which is follow our

safeguarding procedures of reporting the concern and record it so the safeguarding team can act accordingly.

Our computing department and RSE/PSHE curriculum are key in educating students on online safety but through staff training we have a whole school culture of keeping our pupils safe online. We review our online safety provision annually to ensure it is up to date and relevant and in line with DFE online safety guidance, such as the DFE January 2023 guidance on Online Safety.

We send out frequent updates to our parents through our personal development and safeguarding curriculum newsletter and we provide further online resources to our parents through our school website.

The DSL and DDSL receive monthly updates from the National Online Safety website on trends/updated risks online to stay fresh and relevant.

15 Online Filtering and Monitoring

We review our online filtering and monitoring systems annually so that we can ensure we have up to date systems that keep our children safe. We recognise the importance of effective online safety provision and robust filtering and monitoring processes to keep our children safe online, in line with keeping children safe in education 2023.

Currently we use the below systems to support keeping our children safe whilst on our school devices:

Filtering

Our internet filtering is integrated with our internet connection which is connecting to the London Grid for Learning, using software called Web Screen. We carry out regular testing of the filtering processes to check that it is working effectively by using checking packages and carry out pre-planned manual checks. Agilysis oversees the system and the Designated Safeguarding Lead works closely with the Agilysis team to check that effective systems are in place. We report any concerns to the provider.

Device monitoring

To monitor the use of our school devices, both in school and devices that are loaned out to home, we are monitoring using Securus monitoring software. This provides monitoring of all activity on the devices including internet searches, emails, chat and anything that is typed at the key board. It will raise alerts with the safeguarding team by sending a record of the concern with the associated details, such as device name and username.

The Designated Safeguarding Lead and Agilysis regularly review the alerts systems. When concerns are identified the safeguarding team will investigate the concern and respond to it appropriately in line with the safeguarding and child protection procedures outlined in this policy.

Classroom screen monitoring

We use a package called AB tutor to enable the class teacher to monitor all computers in a given classroom when they are leading a lesson. The teacher monitors the usage of the computers and takes control of the devices where needed. This is to enable effective classroom teacher monitoring.

We review our systems annually to identify any new or updated software packages that will strengthen our systems further. We recognise the need to continually review and keep up to date with the evolving online landscape.

We review our systems, processes and provision in line with the 'Meeting digital and technology standards in schools and colleges' guidance March 2023.

Education, Support and Training

We provide staff training annually on the use of filtering and monitoring so that staff understand their roles and responsibilities in regard to keeping children safe online when using school devices in school.

In School

Staff responsibilities include:

- Setting clear expectations and rules around use of devices in a lesson, in line with our behaviour expectations, school ethos and acceptable use policy
- Maintain a high presence in the classroom, monitoring the use of devices
- Utilising AB tutor to support their monitoring of school devices
- Restricting all use of student own devices as we cannot safeguard them effectively on their own devices in the same way we can on school devices. Any such use must be under exceptional circumstances and closely monitored. Students are not allowed to use their mobile devices around site without authorisation, any such use will result in a confiscation.
- Plan lessons carefully to safeguard students from harmful content
- Consider what harmful material may be associated with a particular task or topic
- If any concerns are identified then the staff member must react fast and use the principals of CARE – Communicate, Act, Record and Evaluate. If a student is accessing unsafe content, then the teacher needs to restrict the computer access and call for a member of the safeguarding team.
- The safeguarding team will investigate concerns and apply the safeguarding and child protection policy to deal with any concerns and involve external agencies where required. The safeguarding team will keep detailed records of the concern, the action taken and any follow up support and intervention, such as referrals to PREVENT.
- Maintain a culture of continual learning with regards to online safety.
- Students and staff to understand the acceptable use policy for devices and internet
- Staff to educate students on the risks associated online and how to stay safe online, in line with online safety guidance DFE 2022.
- Parents to be provided with support materials to help keep their children safe online at home.

At home

The school's filtering software does not work when students use their school devices at home on their own WIFI network, unless the student is accessing the internet through our VPN. Therefore, we strongly advise parents set up their own filtering and parent controls. Further information can be found on the NSPCC website using links below and see appendix two for further links to support.

Keeping children safe online | NSPCC

Use Parental Controls to Keep Your Child Safe | NSPCC

The Securus monitoring software does remain operational when a device is at home as it continues to monitor the usage of the device and it will send alerts to our safeguarding team when connected to the internet.

The alerts are monitored during school working hours from 8:45 until 3:15pm. Alerts that are received outside of the working hours will be reviewed and dealt with, as appropriate, during the next school day. Securus alerts are not monitored during holidays, weekends or evenings, but they will be reviewed when the school is next open.

It is a parental responsibility to monitor the use of devices at home and keep their children safe online. Parents must not assume that school are monitoring the devices at all times as this is not the case. Parents must not assume that their child is safe on a school device at home. Children are at risk on school devices at home like any other devices, we have monitoring software but the software does not prevent access to harmful content. Monitoring software is not the same as filtering software. Parents need to restrict the internet content and place parental locks on to try and prevent children access such content.

Parents should consider placing internet access devices in public areas of the house to promote openness and increase the opportunities to monitor the device usage.

Parents need to consider devices such as game consoles, mobile phones, tablets and smart devices, such televisions.

Education:

We provide students with education on online safety, filtering and monitoring in Computing lessons and PSHE/RSE lessons. This is reviewed annually as part of our annual online safety provision audit in line with DFE guidance for online safety 2023.

The Designated Safeguarding Lead is the lead on the school's filtering and monitoring systems and processes, online safety and the training and education.

We recognise that our children with special educational needs and disabilities are vulnerable to being unsafe online and we have considered this in the online safety curriculum planning and delivery to provide them with education that meets their needs. Staff who teach our core curriculum group have received additional training and guidance around online safety, filtering and monitoring.

16. Online Safety Support Links

Online Safety – Support for Children

Childline | Childline for free and confidential advice

Report Harmful Content - We Help You Remove Content to report and remove harmful online content

CEOP Safety Centre for advice on making a report about online abuse

Online Safety – Parental Support

Parents and Carers Toolkit | Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Common Sense Media: Age-Based Media Reviews for Families | Common Sense Media provide independent reviews, age ratings, & other information about all types of media for children and their parents

Support for parents and carers to keep children safe online - GOV.UK (www.gov.uk) about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Information, Advice and Support to Keep Children Safe Online (internetmatters.org) provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

NWG-MCF-Parents-Leaflet.pdf (mariecollinsfoundation.org.uk) Marie Collins Foundation – Sexual Abuse Online

Home (lgfl.net) provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stop It Now! UK and Ireland | Preventing child sexual abuse can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

The Lucy Faithfull Foundation | Preventing Child Sex Abuse can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

CEOP Education (thinkuknow.co.uk) provides support for parents and carers to keep their children safe online

Parent Zone | At the heart of digital family life provides help for parents and carers on how to keep their children safe

Talking to your child about online sexual harassment: A guide for parents | Children's Commissioner for England (childrenscommissioner.gov.uk) This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour for learning policy
- Staff disciplinary procedures
- Data protection policy
- Complaints procedure
- ICT and internet acceptable use policy
- Anti-bullying policy
- The Prevent policy and action plan