St Joseph’s Catholic Primary School

Online Safety Policy

September 2023

Online Safety Policy

Introduction

At Rawmarsh St Joseph's School, we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

Statement of intent

Rawmarsh St Joseph's School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

- Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

What is online safety?

In simple terms, online safety refers to the act of staying safe online. It is also commonly known as internet safety, e-safety and cyber safety. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets. The internet is an incredible resource with the ability to allow children and young people to learn new things, be creative and connect with each other. But there will always be risks present when using the internet, and these risks are always changing. That’s why it is important to keep up-to-date with issues concerning using the internet. Working in partnership, our parents and the school’s role in our children’s online safety is crucial, so we can be there to help avoid these risks turning into problems.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Blogs and Wikis
- Podcasting
- Multimedia
- Gaming
- Mobile devices

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Rawmarsh St Joseph’s, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Parent Agreement are inclusive of fixed and mobile internet technologies provided by the school.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) ‘Filtering and monitoring standards for schools and colleges’
- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2023) ‘Keeping children safe in education 2023’
- DfE (2023) ‘Teaching online safety in school’
- DfE (2022) ‘Searching, screening and confiscation’
- DfE (2023) ‘Generative artificial intelligence in education’
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour and Suspension Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Staff and pupil acceptable use of IT agreements
- Prevent Duty Policy
- Remote Education Policy

Roles and Responsibilities

The governing board is responsible for:

• Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

• Ensuring the DSL's remit covers online safety.

• Reviewing this policy on an annual basis.

• Ensuring their own knowledge of online safety issues is up-to-date.

• Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

• Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

• Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher/DSL is responsible for:

- • Taking the lead responsibility for online safety in the school.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the governing board to update this policy on an annual basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.

- Implementing appropriate security measures as directed by the headteacher.

- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.

- Modelling good online behaviours.

- Maintaining a professional level of conduct in their personal use of technology.

- Having an awareness of online safety issues.

- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.

- Reporting concerns in line with the school’s reporting procedure.

- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

- Staff to only use the device given from school for their own work use.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.

- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

- Reporting online safety incidents and concerns in line with the procedures within this policy.

<u>The Curriculum</u>

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RHE (Relationship and Health Education)
- PSHE (Personal, Social, Health Education)
- Citizenship
- Computing

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the school curriculum.

The teaching of online safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately. Online safety teaching is always appropriate to pupils’ ages and developmental stages.

The DSL (Designated Safeguarding Lead) is involved with the development of the school’s online safety curriculum.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies, such as informing parents/carers, a teacher or trusted staff member, or an organisation such as Childline/CEOP report abuse button.

As a school, we endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

Online safety guidelines and the SMART rules: Be SMART on the internet.

- SAFE
- MEETING
- ACCEPTING
- RELIABLE
- TELL

These will be prominently displayed around the school to remind children of the importance of keeping safe when using the Internet.

Equal Opportunities- Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety.

Internet activities are planned and well-managed for these children and young people.

Staff Training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Staff will have regular staff meetings to inform them of any relevant updates in regards to online safety.

All staff are aware of the procedures that they must follow when reporting online safety concerns. Staff are to report any concerns to the DSL and record any incidents on the school's Child Protection Online Management Systems (CPOMS).

Staff are required to adhere to the Staff Code of Conduct (APPENDIX 1) at all times, which includes provisions for the acceptable use of technologies and the use of social media.

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Educating Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents' evenings
- Class Dojo
- Newsletters
- Parent Meetings/E-safety Events

Parents are sent a copy of the Pupil Agreement Form at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

(Appendix 2)

Security, Data and Confidentiality

Staff may, in some circumstances, use cloud based storage, which is password protected to store and access information conveniently.

Staff should be aware of their responsibilities when accessing sensitive school data.

School data will only be accessed by staff, using their own username and password.

School data will not be duplicated onto personally owned equipment.

Portable devices are encrypted and data can only be accessed using a secure log in.

Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.
The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour and Suspension Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network security

St Joseph's School has an agreement with JMat who securely provide our internet services. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.

JMat provide security against any cyber threats. The server is also backed up off site every day.

All members of staff have their own unique usernames and private passwords to access the school's systems.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the incident should be reported immediately to the teacher/DSL and then passed on to the ICT technicians at JMat.

Managing email

The use of email within school is an essential means of communication for staff. Staff must use the schools approved email system for any school business. Staff must inform the Head if they receive an offensive or inappropriate e-mail.

Use of personal devices

The school allows staff to bring in personal mobile phones and devices for their own use during designated times. These are not to be used at any time whilst children are present.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action as set out in the behaviour policy. This may include discussions with parents, exclusion and reporting the child's access to the respective organisations/companies.

Personal use of social networks

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The School Website

The Head Teacher is responsible for the overall content of the school website. They will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the Photograph Consent Form are met.

Safe Use of Images

Taking of Images and Film

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment such as mobile phones and cameras, to record images of pupils, this includes field trips. The school's ipad devices should be used for this purpose.

Publishing pupil's images and work

All parents/carers will be asked to give permission to use their child's work/photos in publicity materials, on the school website or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents need to inform the school if there are changes, complete a new form, and the previous one will be destroyed.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on the school website, Class Dojo or any other school based publicity materials.

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops.

Misuse and Infringements

Complaints

Complaints or concerns relating to online safety should be made to the Head Teacher Miss C Marsden (following the complaints procedure policy).

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head Teacher/ DSL.

Deliberate access to inappropriate materials by any user will lead to the incident being recorded on CPOMS, and depending on the seriousness of the offence further action may take place; investigation by the Headteacher/Diocese. Staff are aware that misuse or misconduct could lead to disciplinary action.

Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the Headteacher who decides on the best course of action in line with the relevant policies, which include the Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.

Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members.

Where there is a concern that illegal activity has taken place, the Headteacher will contact the police.

Responding to specific online safety concerns

Cyberbullying

At Rawmarsh St Joseph's we do not tolerate Cyberbullying against both pupils and staff. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur with reference to the school behaviour policy.

Code of Practice for pupils

Pupil access to the Internet is through a filtered service provided by JMat, which should ensure resources are safe and secure whilst being used.
In addition, internet access on the school iPads and any other device connected to the school network is automatically also filtered by the web filter.

The following key measures have been adopted by Rawmarsh St Joseph's School to try to ensure that our pupils do not access any inappropriate material:

- Pupils using the Internet will be working in highly-visible areas of the school and will need staff permission before they access the Internet;
- All online activity is for appropriate educational purposes and is supervised
- Pupils will, where appropriate, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils in Key Stage 2 are educated on the safe and effective use of the Internet, through a number of selected programmes and lessons
- The use of mobile phones by pupils is not normally permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff

All pupils will sign a ‘Pupil Code of Conduct’ as outlined in Appendix 2. This involves using online technology inside and outside of school and also whilst accessing online learning through Microsoft Teams at home

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2024.

Any changes made to this policy are communicated to all members of the school community.

We are aware that technology and the potential risks are forever changing; therefore, amendments to this policy will be made if needed in accordance to the new guidance/regulations.

APPENDICES

APPENDIX 1: Staff Code of Conduct

Staff have agreed to the following Code of Conduct:

- *Pupils accessing the Internet should be supervised by an adult at all times*
- *All pupils are aware of the rules for the safe and effective use of the Internet*
- *Websites used by pupils should be checked beforehand by teachers where possible to ensure there is no unsuitable content and that material is age-appropriate*
- *Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to Christie Marsden/ Anna Smith*
- *In the interests of system security, staff passwords should only be shared with the network manager*
- *Teachers are aware that the JMat system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users*
- *Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these*
- *Photographs of pupils should, where possible, be taken with a school camera/iPad and images stored on a centralised area on the school network/password protected internet storage, accessible only to teaching staff.*
- *School systems may not be used for unauthorized commercial transactions*

All staff will be asked to sign the 'Code of Practice for Staff' and these will be stored securely in their staff folders in school.

APPENDIX 2: Pupil Code of Conduct
Pupils have agreed to the following Code of Conduct:

PUPIL CODE OF CONDUCT FOR ONLINE LEARNING

- I will have an adult supervise me whilst using Zoom at home
- I will not share my passwords with anyone except my parents and carers
- I will mute my microphone unless my teacher tells me to unmute it
- I will not mute anyone else's microphone
- I will not share my screen unless my teacher tells me or press the 'take control' button
- I will follow the school rules at all times whilst using Zoom
- I will only talk to my teacher using the chat option if I need to ask a question, I need help or my teacher has given me an instruction to do so
- I will not set up a Zoom meeting or talk to other pupils on chat without the teacher present
- I will use my parents/carer's email (when one is needed) under their supervision

PUPIL CODE OF CONDUCT FOR USING ONLINE TECHNOLOGY

- I will ask permission from a member of staff before using the internet in school
- I will only use my login and password on educational websites such as Times Tables Rock Stars
- I will not share my login in details with anyone else
- I will not access other people's files/work
- I will use the devices only for school work and homework
- I will not bring devices into school unless I have permission
- The messages I send will be polite and sensible using kind words only
- I will not give any personal details to anyone online
- To help other pupils and myself, I will tell a teacher if I see anything I feel is inappropriate or I receive messages I do not like
- I understand that the school may check my computer files and may monitor the Internet sites I visit

All parent/carers will be asked to sign the 'Code of Practice for Pupils' and these will be stored securely in school.