Online Safety Policy

Date of last review:	2024	Review period:	3 Years
Date of next review:	2027	Written by:	Rebecca Garratt
Type of policy:	Non-Statutory	Committee:	FGB
Signature:			

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

- Identify and support groups of pupils that are potentially at greater risk of harm online than others

- 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 and smart technology (which we refer to as 'mobile phones')

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key 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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **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 them 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

2. Legislation and guidance

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

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

- [Relationships and sex education](#)

- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying 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 takes into account the WFS Progression Steps and the National Curriculum computing programmes of study.

.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will 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 governing board will also make sure all staff receive regular online safety updates (via email, 7 minute briefings 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 governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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 their safeguarding needs.

The governor who oversees online safety is the safeguarding governor

All governors will:

- Ensure 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)

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

- Ensure 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

The headteacher 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 designated safeguarding lead (DSL) and deputies 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 ensuring 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 ensure 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

- Working with the IT manager to make sure the appropriate systems and processes are in place

- Working with the headteacher, IT 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

- 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 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 headteacher and/or governing board

- 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.

3.4 The IT manager

The IT 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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's IT 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 half termly 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 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.

3.5 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

- Knowing that the Headteacher is responsible for the filtering and monitoring systems and processes

- 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

  ➢ Search terms entered

  ➢ Bandwidth usage

  ➢ Email accounts

  ➢ Telephone calls

  ➢ User activity/access logs

  ➢ Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above

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

Our governing board is responsible for making sure that:

➢ The school meets the DfE's [filtering and monitoring standards](#)

➢ Appropriate filtering and monitoring systems are in place

➢ Staff are aware of those systems and trained in their related roles and responsibilities

For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns

The headteacher will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

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

- 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

- 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'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers 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

Parents/carers 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 resource sheet – 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 – curriculum content

Pupils will be taught about online safety as part of the curriculum both through the WFS Progression Steps and National Curriculum Computing. Staff will plan timetabled learning and respond at any point of need, as questions or as any issues arise. Pupils will be taught at in an age-appropriate way at their individual levels of understanding, and learning will complement wider understanding within

- Relationships education & Relationships and sex education including online safety and harms:
  - what positive, healthy and respectful online relationships look like
  - the effects of their online actions on others
  - how to recognise and display respectful behaviour online

- Health education

- Citizenship explores:
  - freedom of speech
  - the role and responsibility of the media in informing and shaping public opinion
  - the concept of democracy, freedom, rights and responsibilities

- Computing covers the principles of online safety at all key stages, reflecting the different and escalating risks that pupils face including:
  - how to use technology safely, responsibly, respectfully and securely
  - where to go for help and support when they have concerns about content or contact on the internet or other online technologies

The curriculum offer and learning development adheres to the underpinning knowledge and behaviours set out in the ***DfE Guidance 'Teaching online safety in schools'** (*updated January 2023).

Underpinning knowledge and behaviours for pupils

- How to evaluate what they see online

- How to recognise techniques used for persuasion

- Online behaviour
- How to identify online risks
- Online media literacy strategy
- How and when to seek support
- Online media literacy strategy

Teaching about harms and risks

- How to navigate the internet and manage information
- Age restrictions
- How content can be used and shared
- Disinformation, misinformation, malinformation and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design
- Privacy settings
- Targeting of online content (including social media and search engines)

How to stay safe online

- Abuse (online)
- Online radicalisation
- Challenges
- Content which incites
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication

Wellbeing

- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online versus offline behaviours
- Reputational damage

5. Engaging and educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website (this contains PowerPoints addressing various areas with a clear voiceover to support parents). Twice yearly internet safety workshops provided. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use

Opportunities may be provided to co-design programmes to reflect any emerging issues parents and pupils are hearing about or facing online.

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

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health, careers and economic (PSHCE) 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).

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

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

See searching, screening and confiscation policy. The headteacher, and any member of staff authorised to do so by the headteacher, 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

Pupils and staff at Russell House have the same rights to be safeguarded and protected outside of school hours and, as such, staff are permitted to act within the procedures listed in this policy.

1. *If a member of staff believes a pupil has a prohibited item, they must first ask the pupil to hand it over.*
2. *If the child refuses to, a member of SLT must be contacted.*
3. *A member of SLT and a member of staff will take the pupil to a suitable area eg: office*
4. *The pupil must be asked consent for the search – if they say no, a search cannot take place and parents must be contacted immediately as we have a suspicion of a prohibited item.*
5. *If the pupil agrees, then they can be searched.*
6. *Wherever possible staff of the same sex should carry out the search*
7. *The search can be of bags, lockers or the pupil. The pupil must not be asked to remove any clothing other than outer clothing (clothing not work wholly next to the skin)*

Under common law, school staff have the power to search a pupil for any item if the pupil agrees. The member of staff should ensure the pupil understands the reason for the search and how it will be conducted so that their agreement is informed.

Pupils' possessions can only be searched in the presence of the pupil, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately.

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 Headteacher 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 & searching, screening and confiscation policy

Any complaints about searching electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (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 Bard.

WFS 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.

WFS will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

See ICT & Internet acceptable use policy. All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement (if cognitively able to do so) regarding the acceptable use of the school's ICT systems and the internet. Visitors will abide by the notice on the access slip.

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 and restrict access through filtering systems where appropriate.

8. 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

- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use – see policy.

Whilst devices provided for you are intended for the sole purpose of conducting your work whilst at WFS, Staff are permitted to occasionally use school ICT facilities for personal use, for example online shopping. This is subject to certain conditions set out below. This permission must not be overused or abused. The network manager may withdraw or restrict this permission at any time and at their discretion.
Due to the sensitive nature of materials available to you this benefit strictly does not extend to anybody else, including immediate family members.

Personal use is permitted provided that such use:

Does not take place during class time

- Does not constitute 'unacceptable use', as defined in section 4

- Takes place when no pupils are present

- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Personal devices should be kept secure and out of sight. They should not be used in live classrooms but may be used in PPA or Staff workrooms when on breaks. For emergency contact purposes (for example from your children's childcare provider) you may use the main school number and your extension number, alternatively reception staff will always pass along any urgent messages. On rare occasions permission can be sought from the Headteacher to have their personal phone o their person but not in view of pupils.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media to protect themselves online and avoid compromising their professional integrity.

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

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 behaviour, ICT and internet acceptable use, safeguarding and mobile phone policy. 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 code of conduct. 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.

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 7 minute briefings).

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, 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.

12. Monitoring arrangements

Analysis of CPOMS data.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy

- Behaviour policy

- Staff disciplinary procedures

- Data protection policy and privacy notices

- Complaints procedure

- ICT and internet acceptable use policy