Online Safety Policy

Date	October 2025
Written By	Lulu Stanier-Martin/Lauren Steels
Approved By	Joe Creswick
Date Approved	October 2025
Review Date	October 2026

This policy applies to all stakeholders within Ridgeway School

Note: Children includes everyone under the age of 18. At Ridgeway, our young people may stay in our sixth form provision until they are 19 years of age. Due to their vulnerability, this policy will continue to be used until they leave Ridgeway. When we refer to 'children' and 'school' in this policy, we also cover 'young adults' and 'sixth form. This policy also applies to pupils in the Early Years Foundation Stages (EYFS).

Introduction

Ridgeway has good, strong processes in place to ensure the online safety of all of our community, especially our pupils and staff. We know that technology enables us to do lots of amazing things: communicate, learn new skills, develop existing skills and share information, but we also know that working online comes with a number of risks, and that the nature of these risks are constantly evolving and changing. Our staff survey reflects that our staff feel confident that we teach children and young people how to be safe online at Ridgeway; we work to continually educate our whole school community to use technology in a safe and empowering way.

The purpose of this policy

This policy aims to clarify the risks of online safety, and the proactive measures that we take to keep ourselves safe online. If we have concerns about anything to do with online safety, we want pupils and staff to know how to identify, intervene and escalate these concerns in a clear, supportive and appropriate way.

Every pupil at Ridgeway has an Education, Health and Care Plan (EHCP), so we know that they need sensitive, specialised support in all areas, including online safety. This policy reflects this need.

What are the risks?

Our approach to online safety is based on addressing the following categories of risk, as per the current version of
Keeping Children Safe in Education:

- **Content**: being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

How do we keep ourselves safe online at Ridgeway?

- At Ridgeway, we encourage staff and pupils to have ongoing conversations about internet use, recognising that openly talking about what children and young people do online is the best way to understand their experiences and feelings about being online.

- Staff work to give pupils lots of opportunities to engage with technology in positive ways, including use of iPads, laptops, interactive white boards and digital cameras. We are always looking for exciting augmentative ways to access and use technology to enhance our learning, such as BeeBots and VR headsets.

- At Ridgeway, all pupils follow our purpose-written Ridgeway curriculum. Online safety is fully integrated into our curriculum; it is built into our 'understanding the world' and 'PSED' areas of learning strands. We often discuss the importance of teaching online safety for all ages and at all levels of learning, to help staff understand what this might look like for their pupils' specific needs – see for example the document in Appendix One. A large number of supportive resources to aid teaching and learning are saved in our shared teachers' online drive.

- Teachers are expected to deliver a minimum of two online safety lessons per half term – this is likely to need to increase as pupils become more independent and explorative users of the internet. The content of these will be based on individual need, individual stages on the curriculum and the topic breadth grid. At least one observation related to online safety should be recorded per pupil per half term on Evidence for Learning, using the 'online safety' tag. Where appropriate, pupils in Key Stage 3 and above are given increasing opportunities to use laptops to complete classwork. Staff must recognise that at these ages pupils are increasingly likely to use their own devices and have their own social media accounts. It is vital that staff take time to discuss with pupils how they access the internet and continually offer teaching that is responsive to individual pupil need.

- We recognise that due to all our pupils having individual additional needs, they will all access technology and the internet in unique ways, and that their learning connected to online safety might not progress in a linear way. It is important that teachers have the flexibility to understand and respond to individual pupil need regarding online safety, in correspondence with their identified strengths and needs, considering the risks highlighted above and with reference to the curriculum.

- We ensure that we are compliant with the Department for Education's filtering and monitoring standards. Our DSL and IT team work together to ensure that all appropriate safety settings and filtering arrangements are applied to all devices that are used around the school and college, including laptops and iPads. This provision has an annual strategic review, and ongoing operational checks. We currently use Virgin Broadband, a provider with an excellent reputation. Our filtering blocks child sexual abuse content, terrorism content, adult content and offensive language. If any staff or pupils try to search for any blocked content or access a website of concern, a notification is sent to the Designated Safeguarding Lead (DSL) and Network Manager, to allow them to consider whether any further action is necessary.

- We use reputable, secure systems to communicate with our wider community, including our Ridgeway email addresses, Parent Mail and Class Dojo.

Specific information

Acceptable internet use

- Staff are all expected to sign an agreement regarding appropriate use of IT and the internet and must comply with this. This is signed as part of induction and then again, every September.
- Pupils and students from KS3 upwards are expected to sign an accessible agreement regarding using the internet, if appropriate considering their level of cognition (see Appendix Two). Students at the Sixth Form keep their mobile phones in their bags during the day when not in use.

- Visitors will be expected to read and agree to our terms on acceptable use of IT, if relevant.
- Use of Ridgeway internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- The filtering arrangements described above enable monitoring of the websites visited by all of those using the internet at Ridgeway to ensure they comply with our acceptable internet use requirements.

Cyberbullying or online abuse

- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic or misandrist messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography
- Staff work to help pupils to understand that bullying and abuse can happen online as well as in real life, to understand how this might look.
- Staff encourage pupils to understand and have strategies of how to respond and then report any concerns, whether they relate to themselves or others.
- Any safeguarding concerns must be reported to the safeguarding team and using CPOMS, as per the safeguarding and child protection policy.
- If illegal, inappropriate or harmful material has been spread among pupils, we 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.
- The safeguarding policy contains specific guidance around youth produced sexual imagery.
- The anti-bullying policy also considers cyber-bullying.
- Online abuse is covered in initial safeguarding training and is constantly reflected on through weekly safeguarding update emails.

Examining electronic devices

Education 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. 'Good reasons' could be that the image or file could cause harm, disrupt teaching, or breach school rules.

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Generative artificial intelligence (AI)

We will take steps to prepare pupils for changing and emerging technologies, such as generative AI, and will endeavour to teach pupils how to use them safely and appropriately. We will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI. We will make use of any guidance and support that enables a safe, secure and reliable foundations before using more powerful technology such as this.

Personal devices and mobile phones

- Some pupils bring personal devices into school to use whilst on bus or taxi journeys. This is acceptable, but families must be aware that Ridgeway cannot be responsible for ensuring the safety of these devices.
- Pupils are supported to keep personal devices in a safe place throughout the day, for example the office are able to store mobile phones.
- Pupils must not use personal devices throughout the day, unless there is a specific need for them as a learning tool, for example as a communication aid.
- Sixth form students are allowed to bring their phones to college with them; staff work with students to teach them how to use their phones to aid their independence, for example using calculators, accessing shopping apps, taking images as aide memoirs, following QR codes, or calling for help when travelling independently.

Roles and responsibilities

All staff will:

- be aware that children are at risk of online abuse; that technology is a significant component in many safeguarding and wellbeing issues; and that in many cases, abuse and other risks will take place concurrently both online and offline
- support and encourage pupils to engage positively with technology and internet access
- supervise and monitor pupils whilst they access the internet, with an awareness that pupils might access inappropriate or harmful material deliberately or accidentally
- ensure that pupils only access the internet via a pupil login, not a staff one (this is due to different levels of filtering)
- report any concerns around online safety, including sending of nude or semi-nude images, cyberbullying and sexual violence or harassment, using CPOMS, as per the safeguarding policy
- adhere to relevant policies and training alongside this policy, such as GDPR, Prevent, code of conduct, data protection, confidentiality and use of IT agreement

- be aware that if they misuse IT, they may be subject to disciplinary procedures
- not have their mobile phones on their person whilst they are in contact with pupils, unless for one of two reasons:
    - o Expecting a personal phone call, such as a GP appointment, with specific permission from the leadership team
    - o When supporting pupils offsite, for safety and contact purposes

- never take photos of pupils on their personal devices (mobiles or cameras)
- only use smart watches or Fitbits **as watches** around the pupils
- ensure that they use any work devices safely and appropriately, as per the Use of IT agreement, which includes expectations around locking devices
-
- access GDPR training on joining Ridgeway, and again yearly, and actively implement this
- share job vacancies on social media if they want to, but apart from this, **no** information about Ridgeway will be posted on personal social media
- ensure that their social media is either set as private, or if public, that content is appropriate considering their position of responsibility

- maintain professional boundaries around communicating with pupils online:
- Never communicate with pupils via social media platforms

- Only use the Ridgeway email system to communicate with pupils and only communicate with them during school hours

- Only use Class Dojo or Ridgeway email to communicate with parents

- Never pass on personal phone number / email address to parents/carers

- Maintain professional boundaries in all emails

- FOR OFFICE-BASED STAFF ONLY: complete a yearly Display Screen Equipment self-assessment and follow guidance about how to support good posture.

The Executive Headteacher & Head of school will:

- ensure that this policy is implemented consistently and effectively throughout Ridgeway
- ensure that the DSL accesses training to enable a good awareness of online safety.

The Designated Safeguarding Lead (DSL) will:

- take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place
- work with relevant staff to address any online safety issues or incidents, and ensure that they are recorded appropriately on CPOMS
- work with relevant staff to ensure that any safeguarding concerns, including incidents of child-on-child abuse, or sexual violence / harassment are managed in line with the safeguarding & child protection policy
- lead on delivering or organising online safety training for staff, including induction, yearly refreshers, ongoing regular updates, and covering Prevent (dealing with extremism and radicalisation, which predominantly happens online)
- share relevant online safety information with parents / carers

- include relevant information about online safety in safeguarding reports to governors
- support the Executive Headteacher in ensuring that this policy is implemented consistently and effectively throughout Ridgeway.

The Network Manager will:

- work with the DSL to ensure that Ridgeway is meeting the DfE filtering and monitoring standards
- put in place an appropriate level of security protection procedures that protects children and young people, without unreasonably impacting teaching and learning
- review and update these systems on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at Ridgeway – including blocking access for pupils and staff to potentially dangerous or extremist sites
- ensure that the Ridgeway IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conduct regular security checks and system monitoring exercises
- work with SLT (predominantly the Business Manager and the DSL) to review Use of ICT / Acceptable Use agreements for all stakeholders
- allocate equipment and track this through an asset register
- liaise with the DSL or Headteacher regarding any concerns that they identify in connection with online safety or cyberbullying.

The Technology & Online Safety Lead will:

- support the leadership team in ensuring that appropriate learning is implemented that gives pupils sufficient knowledge and skills to stay safe online
- support the leadership team in monitoring and evaluating the impact of the teaching and learning of online safety throughout Ridgeway

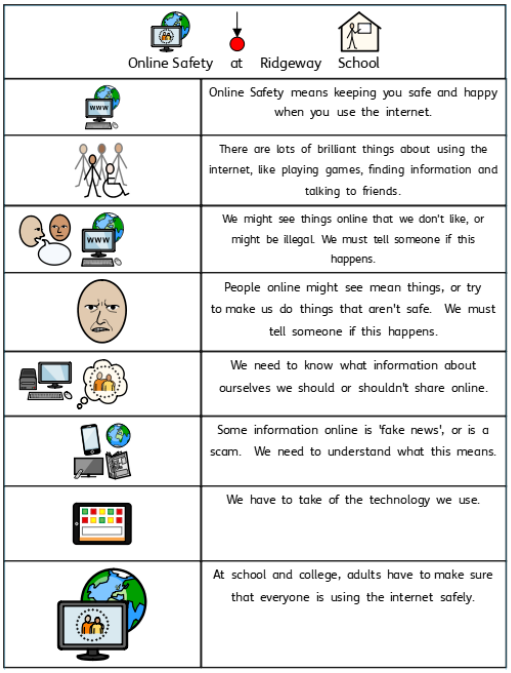
- support the DSL in raising parent/carer awareness
- support teachers to access appropriate and exciting ways of teaching online safety, by promoting resources and developing teachers' knowledge.

Governors will:

- ensure that they have a full understanding of this policy and the school keeps pupils safe online
- hold relevant staff to account for implementing it effectively.

Pupils will:
This is our accessible online safety policy for pupils:

- engage in learning activities about online safety, adapted to their individual needs
- where appropriate, understand that their internet activity is monitored
- follow the Golden Rules or Expect Respect rules whilst engaging with others on the internet
- look after the technology that they use
- use technology in a safe and appropriate way.



Families will:

- share with us any important or relevant information about how their child accesses technology and the internet
- make us aware of any concerns about their child's online safety, to enable us to respond appropriately from a school or college perspective
- engage with updates on Dojo or Parent Mail that are relevant to them
- contact our Network Manager if help is needed to set filters
- take steps to ensure that their child doesn't access inappropriate content.

Legal framework & statutory guidance

Linked national guidance:

- Cyber bullying: advice for headteachers and school staff (DfE, July 2017)
- Filtering and monitoring standards for schools and colleges (DfE, March 2023)
- Keeping Children Safe in Education (DfE, September 2023)
- Preventing and tackling bullying (DfE, July 2017)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE, September 2021)
- Searching, screening and confiscation: advice for schools (DfE, January 2018)
- Teaching online safety in school (DfE, June 2019)
- The prevent duty: for schools and childcare providers (DfE, August 2015)

Linked policies:

- Anti-Bullying policy
- Code of conduct
- Confidentiality policy

- Data protection and use of IT agreement
- Data protection policy
- Remote learning policy
- Safeguarding & child protection policy
- Staff handbook

Equalities & inclusion

Research shows that vulnerable children experience significant benefits from being online. However, they are also more likely to experience online risks. As such, they require very specific support to develop digital resilience to benefit safely. Ridgeway strives to ensure that children and young people all have meaningful access to technology, in a way that accommodates their individual special needs. It is important that online safety teaching is delivered in ways that knowledge these needs and makes online safety accessible for pupils working at all levels.

Safeguarding implications

Technology is a significant component in many safeguarding and wellbeing issues, and we must be mindful that all children are at risk of online abuse. This policy is additional to the Safeguarding and Child Protection policy; any safeguarding concerns raised in connection with online safety should be managed according to the Safeguarding and Child Protection policy.

Appendices

ONE: Online safety at early stages of learning

TWO: Pupil acceptable use agreement

THREE: Online safety risk assessment

FOUR: Prevent specific risk assessment

APPENDIX ONE: online safety at early stages of learning

Online safety at early stages of learning

Children need to learn online safety at all ages, and all stages of learning. Online safety does not just apply to older pupils who use the internet independently; lots of children at early stages of learning use the internet to watch cartoons, films and songs.

The four areas of risk in online safety are identified as content, contact, conduct and commerce. There is more about these in our online safety policy. They still apply to pupils at early stages of learning, just in different ways!

Here are some top tips for what online safety work can look like at early stages of learning:

CONTENT

- Explore fun and safe activities on the internet together, choosing apps and games that allow them to develop skills.
- Model what you do if you see something that you don't like.

CONTACT

- Model kindness online, saying kind words and sending kind messages to others.
- Model consent and respectful sharing practice, for example asking to take photos of them, even if you think they aren't listening to you!

CONDUCT

- Work on cause and effect games, such as apps where you tap the screen to make fireworks explode. This enables them to build an understanding that they can influence what they see on a screen – it doesn't have to happen to them.
- Describe what you are thinking and doing, and if appropriate, ask questions, such as "I wonder what will happen when we tap here?"
- Practise turn taking on the internet.
- Access simple stories and videos about online safety – there are lots on YouTube, and lots are signposted in the Curriculum Resources folder on the Drive.
- Teach them to ask for help when something isn't working how they want it to on a device.

COMMERCE

- It's important to ensure that appropriate safety settings and filters are on all devices used by pupils. Younger pupils have sometimes share things or make purchases inadvertently! They must always be supervised when using technology.

APPENDIX TWO: pupil acceptable use agreement

Using the Internet at Ridgeway

I understand that:

- The internet can help us in amazing ways, but we must follow some rules to stay safe.
- Staff are there to help me learn how to use the internet safely.
- Not everything that I see on the internet is true.
- Lulu, Lauren and Neil make sure that people are using the internet safely, so they will see if I try to do something inappropriate on the internet at Ridgeway.
- If I break these rules, I might not be able to use the internet at Ridgeway.

I know that I must:

- Listen to what staff say, and only use websites or apps that they have agreed to me using.
- Ask for help if I think I have made a mistake online.
- Ask for help if I see something online that I don't like.
- Be kind online: bullying, being mean and bad language is not ok on the internet.
- Not share private information about myself online.
- Not share private information or pictures about anyone else without their consent.
- Not speak to anyone online that I don't know whilst I am online at Ridgeway.
- Not share information about Ridgeway online unless staff have said it's ok.
- Not try to buy anything whilst I am online at Ridgeway.
- Keep my username and password private and safe.
- Take care of all our IT equipment, like laptops and iPads.

I agree to these rules.

Signed:

Date:

APPENDIX THREE: online safety risk assessment

Description	Details	Who?	Mitigating action
Exposure to inappropriate online content	• Commercial – adverts, spam, sponsorship, personal info • Extremist - violent / hateful content • Sexual - pornographic or unwelcome sexual content • Values – bias, racist, misleading info or advice	Children & staff	• Use of IT Agreement • Appropriate filtering • Pupils actively taught how to report concerns about content • Information shared with parents/carers about filtering systems at home • All staff have Prevent training
Inappropriate online contact	• Aggressive - being bullied, harassed or stalked • Sexual – harassment, meeting strangers, being groomed • Values – self harm, unwelcome persuasions NOTE: Ridgeway pupils may be particularly vulnerable to this due to their SEND	Children & staff	• Online Safety policy • Reporting mechanism • A culture where pupils are supported to share worries safely • Appropriate monitoring • Online safety teaching & learning • Work to identify SEND-specific resources
Inappropriate online behaviour	• Commercial – Illegal downloading, hacking, gambling, financial scams, terrorism • Aggressive - being bullied, or harassing others • Sexual – peer harassment, creating and uploading inappropriate material • Values – providing misleading info or advice	Children & staff	• Use of IT Agreement • Safeguarding policy • Infrastructure security • Appropriate monitoring • Online safety teaching & learning • Work to identify SEND-specific resources
Cyber and Information Security	• Data Protection – data loss or compromised • Security Intrusion – information or access is compromised e.g. hack or virus/malware	Staff	• GDPR Policy • GDPR training (including advice on passwords) • Data Protection Officer • Protective systems (anti- virus) • Software updating regime

			• Incident management
Safeguarding	• Staff capability to recognise, respond and resolve issues	Staff	• Training programme including induction, refreshers and weekly safeguarding updates • Use of CPOMS to record information • Senior leadership and Designated Safeguarding Lead responsibilities • Clear lines of escalation • Staff survey to track staff confidence

APPENDIX FOUR: Prevent specific risk assessment

Description	Yes / No	Who?	Supporting action
Does your safeguarding policy make explicit that the school sees protection from radicalisation and extremist narratives as a safeguarding issue?	Yes	DSL	Radicalisation and Prevent are identified in the safeguarding policy, and Keeping Children Safe in Education is referred to for further detail.
Are the lead contact for Prevent responsibilities clearly identified in the policy?	Yes	DSL	Having a large staff team, we are consistent in guiding staff to refer all safeguarding concerns to the DSL or deputy.
Does the policy make explicit how Prevent concerns should be reported within school?	Yes	DSL	We give our staff clear information to report all concerns through CPOMS, which ensures consistency. The DSL remains up-to-date with Central Bedfordshire reporting procedures.
Are Fundamental British Values (FBV) considered in curriculum planning?	Yes	SLT	Our curriculum was designed in-house, and FBV were integrated into the development process. Ongoing development of FBV-related provisions has been part of our School Improvement & Development Plan Diversity has been a significant area of focus and development
Thinking about an incident of radicalisation and/or extremism - has the setting considered specific potential areas of risk?	Yes	SLT	We have a School Emergency Plan on a shared 'emergencies' drive that SLT have accessed to. We have experience in managing SARs, and we have a lockdown procedure in place.
Does the school have clear guidance for visiting speakers?	Yes	SLT	For any external services being sought, we only use known and recommended training providers. When visitors arrive, the office team follow clear procedures to verify their identify. Our premises are currently only used by established local charities that provide disability support, or by groups connected to health or social care partners.
Have ALL staff received appropriate training on Prevent?	Yes	DSL	All staff – including support staff – complete Prevent training as part of their induction. Prevent is also referred to in initial safeguarding training. Relevant updates are shared throughout

			the year in safeguarding update emails, and Prevent is updated yearly. Prevent training is tracked on the Single Central Record.
Does the E-Safety Policy refer to the requirements of the Prevent guidance?	Yes	DSL	This risk assessment is appended to the online safety policy to firmly connect Prevent strategy with online safety. The policy also clearly reflects the need for appropriate filtering that blocks access to dangerous or extremist websites.
Protocols are in place to manage the layout, access and use of any space provided for the purposes of prayer, contemplation and faith facilities.	No		There are no relevant facilities at Ridgeway.
Clear guidance on governing the display of materials internally at the school	Yes	SLT	There is display guidance for classrooms and this is monitored by the senior leadership team. There is not a culture of staff displaying their own materials in the staffroom; this is monitored.