Rivacre Valley Primary School
Online Safety Policy

Online Safety: The Rationale

Our school aims to:

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

Online Safety encompasses the use of new technologies, internet (including social-networking) and electronic communications such as websites, mobile phones and video conferencing (such as Zoom/Teams/Google Meets). It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for all users to enable them to control their online experience.

Roles and Responsibilities:

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

The governing board will coordinate regular meetings with appropriate staff, usually the computing lead, to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). These take the form of Web admin from Schools broadband and Senso Alerting

Currently the HT receives daily alerts from Schools broadband and weekly Senso alerts. This enables the school to monitor what is being searched for and by whom. Senso even provides a screen shot of the page so the context can inform follow up actions.

All governors 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

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

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

- 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 Governing Board.

The Online Safety Coordinator for Rivacre Valley Primary School is **Mrs Walker-Stokes** who works alongside Mrs Kate Docherty who is our Head teacher and DSL.

- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by: Catherine Harper and Chloe Steadman

Teaching and learning

At Rivacre Valley Primary School, we use eAWARE to assess, educate and raise awareness to reduce the vulnerability of children's behaviour online.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

Internet use will enhance learning

- The internet access will be used expressly for pupils and will include filtering appropriate to the age of pupils.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation, both inside and outside of a school context.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems and security will be reviewed regularly with a technician on site every week for half a day.
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.
- Netsweeper and Senso software has been installed on all school laptops and desktops and monitors inappropriate content. This company then contacts school with the risk and details of content found. If a low risk, then this is emailed weekly to SLT. If there is an immediate risk, then school is emailed.

E-mail

- Pupils will not have their own individual e-mail accounts nor will they be allowed to access any personal email addresses they have

Passwords

- All computers need a password to gain access
- All passwords are kept safe
- All staff email accounts have a secure password
- Staff are encouraged to use Google Drive to store school related information.
- All staff laptops are password protected / encrypted.

Software

- All software installed on computers is checked for age appropriate content, depending on the age of pupil accessing it.
- Pupils are taught about software that can be accessed outside of school, and the need for responsibility.

Publishing pupil's images and work

- Where the school uses images of individual pupils, the name of the pupil will not be disclosed.
- Where an individual pupil is named in a written publication, a photograph of the pupil will not be used to accompany the text. If, for example, a pupil has won an award and their parent would like their name to be published alongside their image, separate consent will be obtained prior to this.
- Parents or carers will be asked to give consent for their child's photographs to be published on the school website/social media when their child starts school. This is found on Page 6 and 7 of the school prospectus.

Social networking and personal publishing

- The school will block/filter access to some social networking sites – these will only be used by staff in accordance with the acceptable use policy
- Pupils will be advised never to give out personal details of any kind which may identify them or their location if using social media at home.
- Staff are not allowed to post any comments on social networking sites that relate to the school and/or children/staff.

Managing filtering

- The school will work with the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to DSL or SBM who will take appropriate action
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The HT receives daily alerts from Schools broadband and weekly Senso alerts. This enables the school to monitor what is being searched for and by whom. Senso even provides a screen shot of the page so the context can inform follow up actions.

Managing videoconferencing (Zoom/Microsoft Teams/Google Meets)

- Video Conferencing with a class will only take place during lesson time and not when children are using ICT independently
- Staff must use video conferencing appropriately and report anything that could cause harm.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and ensuring compliance with GDPR
- Children's personal data will be accessed via secure documents on google drive or via secure school systems (Insight / CPOMS).

Policy Decisions

Authorising Internet access

- All staff must read the 'Acceptable Use Policy' (See Appendix 1) before using any school ICT resource.
- All students must read and agree to the 'Pupil Acceptable Use Agreement' (See Appendix 2) and a class charter will be signed.
- Within the school access to the Internet will be supervised. Lower down the school access will only be to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will regularly audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.
- Once an incident report log has been completed, it is shared with the safeguarding lead and SLT through CPOMS and, where appropriate, all members of staff. Safeguarding issues are also discussed at the beginning of professional development meetings.
- All staff have received PREVENT training and will continue to receive regular training in the future. This ensures that all members of our school community recognise the dangers of radicalisation, the impact that this can have on our children and signs to look out for threatening behaviour

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Introducing the Online Safety policy to pupils

- Online Safety rules will be discussed with the pupils at the start of each year.
- Pupils are informed that network and Internet use is monitored.
- Through the use of eAWARE and the development of the Online Safety Policy, pupils will gain knowledge and understanding of why it is important to stay safe and how to go about this.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy on the school website/social media.
- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

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 and economic education, and other subjects where appropriate.
- The school also sends information 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 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.
- 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.

Examination of staff device

Whilst the law dictates that 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, staff at Rivacre Valley Primary school will not handle pupils' devices without a parent present.

Mobile Phones

Mobile phone handed in on arrival – At RVPS children may require access to their mobile phones before and after school. Children do not have access to their mobile phones throughout the school day. On entry to the school each child hands in their device to school staff and these are then collected at the end of the school day.

Most children are compliant with this and it is very rare for a child to keep their phone with them. If staff discover a child has a phone in their possession during the school day they will be spoken with, asked to switch it off and then the phone will be removed and kept until the end of the day. Parents will be notified.

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).

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Appendix 1
Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to read this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Board. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand this forms part of the terms and conditions set out in my contract of employment.

Appendix 2
Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community

- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Appendix 3
Guidance in response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any Online Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to online safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the Online Safety Officer or the Police Liaison Officer.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

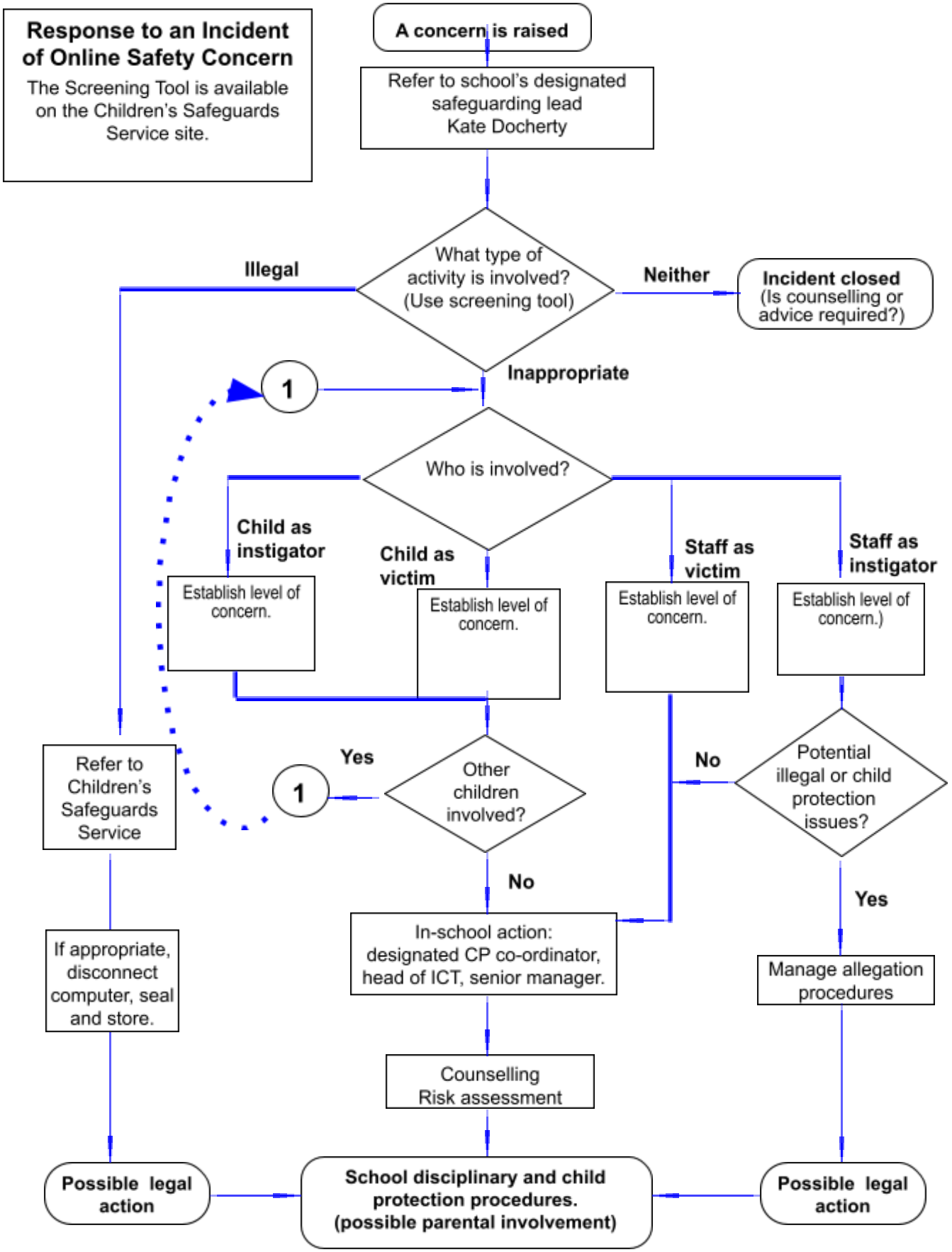
What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches

How do we respond?

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Protection Unit and Designated staff member should be consulted.

As previously stated schools should ensure that relevant policies (Acceptable Use Policy, Behaviour Policy, Bullying Policy, Discipline Policy) are referenced and are considered when dealing with the issues identified.


Response to an Incident of Online Safety Concern
The Screening Tool is available on the Children's Safeguards Service site.
A concern is raised
Refer to school's designated safeguarding lead Kate Docherty
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
1
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern.
Establish level of concern.
Establish level of concern.
Establish level of concern.)
Refer to Children's Safeguards Service
1
Yes
Other children involved?
No
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action