RAVENSCOTE JUNIOR SCHOOL

ONLINE SAFETY POLICY

2024 - 2025

Date of Approval		Date of Review	
March 2024		**March 2025**	
Signed	Amy Wells **Headteacher**	**Signed**	Emily Gibson **Chair of Governors**

Ravenscote Junior School

Online Safety Policy

This policy should be read in conjunction with the Child Protection and Safeguarding Policy, Whistleblowing Policy, Low-Level Concerns Policy, Computing Acceptable Use Policy, Computing Policy and Social Networking Policy.

Computers and the use of the Internet are a valuable resource for learners of all ages. It is increasingly providing the focal point of educational content within the UK. This policy outlines our purpose in providing email facilities and access to the internet and explains how Ravenscote Junior School is seeking to avoid the potential problems that unrestricted internet access could give rise to. The policy also sets out the procedures by which the school will minimise the misuse of computers and associative technology.

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

Providing access to the internet in school will raise educational standards and support the professional work of staff. Internet use will enhance learning so the school internet access has been designed for child use and includes filtering appropriate to the age of the children. Children will be taught what Internet use is acceptable and what is not, they will be given clear objectives for Internet use.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Ravenscote Junior School.

- The headteacher (Amy Wells) has a duty of care for ensuring the safety (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) of members of the school community.
- The headteacher (Amy Wells) is responsible for ensuring that Ravenscote Junior School meets the statutory Filtering and Monitoring standards for Schools and Colleges.
- The designated safeguarding lead has lead responsibility for safeguarding and child protection (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring).
- The day to day responsibility for online safety will be delegated to the Online Safety leads: Natalie Nicholson, Sophie Spooner and Hannah Burrows.

Online Safety Leads:

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

Network Manager

Technical responsibilities are carried out by Mrs Lisa Crouch, who ensures:

- That Ravenscote's technical infrastructure is secure and is not open to misuse or malicious attack
- That Ravenscote meets required online safety technical requirements and any relevant local authority guidance which may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and of the current Ravenscote online safety policy and practices.
- They have read, understood and signed the staff acceptable use policy.
- They report any suspected misuse or problem to the Headteacher or Online Safety leads for investigation, action and sanction.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.

Designated Safeguarding Lead

Should be trained in online safety issues, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and filtering and monitoring).

Children:

- Are responsible for using Ravenscote digital technology systems in accordance with the acceptable use agreement.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be

encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.

Ensuring Internet Access Is Safe and Appropriate

Ravenscote will be responsible for ensuring that the school's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Ravenscote's technical systems will be managed in ways that ensure they meet recommended technical requirements.
- There will be regular reviews and audits of the safety and security of academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and secure password by Lisa Crouch who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school systems, used by the Network Manager must also be available to the Headteacher or another nominated senior leader and kept in a secure place.
- Lisa Crouch is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered and monitored for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- All staff are provided with a copy of "Filtering and Monitoring at Ravenscote Junior School" to ensure that they understand how to keep pupils safe online and wat to do if they have concerns regarding what children are accessing (see appendix A).
- Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. This is in line with the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- School/academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Authorising Internet Access

All staff must read and sign the 'Computing Acceptable Use Policy for Staff'. The school will maintain a current record of all staff and pupils who are granted access to school systems. Parents will be asked to sign and return an Internet use consent form.

Any persons not directly employed by the school will use a Guest log-in to access the internet from the school site, thereby restricting access to the school network. When joining this network, guests will be prompted to agree to an 'Acceptable use of School Computing Resources' statement.

Staff and Online safety policy

All staff will be given the school Online Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Ensuring Online Safety for children:

The education of pupils in online safety is an essential part of Ravenscote's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PSHE, this includes children being able to know and identify the four categories of risk – "Content, Contact, Conduct and Commerce".
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Children are taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. This is in line with the additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Children are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside Ravenscote.
- Staff should act as good role models in their use of digital technologies.
- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Ensuring Online Safety for parents and carers:

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school/academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Ensuring Online Safety for the wider community:

Ravenscote will provide opportunities for local community groups/members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards relatives as well as parents.
- The school/academy website will provide online safety information for the wider community.

Ensuring Online Safety for staff:

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Leads and DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Online Safety Leads and DSL will provide advice/guidance/training to individuals as required.

Social Networking

The school will control access to social networking sites and consider how to educate children in their safe use. Children will be advised never to give out personal details of any kind which may identify them, their friends or their location. Children and parents will be advised that the use of social network spaces outside school brings a range of dangers. Children will be advised to use nicknames/avatars when using social networking sites.

School Website

Our school web site is intended to:

- provide accurate, up-to-date information about our school
- promote the school.

School website address: www.ravenscote.surrey.sch.uk

Children's full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of children are published on the school web site. Child image file names will not refer to the child by name. Parents will be clearly informed of the school policy on image taking and publishing.

Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

Emerging Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff & other adults				Children			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school/academy	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones/cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices		X					X	
Use of personal email addresses in academy, or on academy network	X							X
Use of academy email for personal emails				X				
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs		X					X	

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and children or parents/carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official (monitored) school/academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Children should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school/academy website and only official email addresses should be used to identify members of staff.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (UKGDPR). Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The academy must ensure that:

- It has a Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.

It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a "retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.

- It provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice.
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum).
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.
- Device must be password protected.
- Device must be protected by up to date virus and malware checking software.
- Data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understands their rights and know how to handle a request whether verbal or written.
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school/academy personal data to personal devices except as in line with school policy.

- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

If you have concerns about a child's conduct, refer to the Child Protection and Safeguarding Policy. Actions and consequences may include: informing parents/carers, referral to the head teacher or removal of internet access rights.

If you have concerns about an adult's conduct, refer to the Whistleblowing Policy and Low-level Concerns Policy.

Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos.

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix A

Filtering and Monitoring at Ravenscote Junior School

Learn about our school's filtering and monitoring systems and how you can help to keep pupils safe online and know what to do if you have concerns about the content that pupils are accessing.

What is filtering and monitoring?

Filtering systems block access to harmful websites and content.

Monitoring systems:

- Identify when someone searches for or accesses certain types of harmful online content on school devices
- Identify who is searching for or accessing the harmful content
- Alerts the school about it so we can intervene and respond
- **Don't** block access to harmful content

We're all responsible for filtering and monitoring

- No filtering and monitoring software is perfect:
- It might not be aware of all the websites that contain inappropriate content
- Abbreviations or misspellings in a search engine may slip past the software
- Inappropriate content may be found on websites considered 'safe'

You can help to make sure the internet is used appropriately by:

- **Monitoring** what pupils are accessing on devices during school hours (e.g. by looking at their screens when using computers during lessons)
- **Teach** children about responsible digital behaviour, ethics, and the consequences of inappropriate online actions.
- **Alerting** **Lisa Crouch** if you become aware that content is not being filtered
- If you have concerns about what a pupil is accessing online, always raise it with **Natalie Nicholson**, if she is not available, speak with any of the DSL Team.

Inappropriate content includes:

- Illegal content (e.g. child sexual abuse)
- Discriminatory content (e.g. sexist, racist or homophobic content)
- Sites that promote drugs or substance abuse
- Extremist content (e.g. the promotion of terrorism)
- Gambling sites
- Malware and/or hacking software
- Pornography
- Pirated material (copyright theft)
- Sites that promote self-harm, suicide and/or eating disorders
- Violent material

What systems do we use?

Keeping Children Safe in Education 2023 states that all schools should have appropriate filtering and monitoring systems in place.

We have the following systems in place:

Filtering: LGFL

What is it? Content control – blocking or allowing content using URLs, keywords, content categories

What does it do? **Protects** from harm (but no guarantees, not 100%), **minimises distractions** from learning, **needs to be balanced** – protection v over-blocking, tends to be **reactive**.

Monitoring: SENSO and staff

What is it? Supervision (physically or via tech) of what children are accessing

What does it do? Protect from online bullying, **verify** learners are acting responsibly and learning acceptable online behaviour, **ensure** the filtering **system is working** well, **provide** a **safe** place to learn from mistakes.

Our School Response to Filtering and Monitoring Alerts.

- When accessing any school device, all children must be logged into the RDP to enable any alerts to identify them my name.
- On the rare occasion when they are unable to use a device when logged into RDP (due to a piece of software not running in RDP or when using the student iPads), class teachers are aware of which children are using devices.
- If anyone attempts to access blocked content, SENSO issues an alert which goes directly to Lisa Crouch (IT Technician), Amy Wells (Head and DDSL) and Natalie Nicholson (DSL).
- This alert is acted on immediately, an e-mail is sent to the class teacher to follow up with the child later. If the child is still working on the school device, the alert can be discussed with them immediately.
- If the alert is triggered by a monitored child or is of a racist, sexual or extremely graphic nature then it will be logged onto CPOMS for further follow up.
- A weekly report is run each week by Lisa Crouch and logged in the following location - P:\Safeguarding\Online Monitoring Filtering Reports\2023-24
- The reports are viewed in weekly DSL meeting to look for patterns and trends, and identify whether any further action needs to be taken or whether any further words/websites etc may need to be blocked.
- Lisa Crouch is responsible for maintenance and review of the software.
- Amy Wells(headteacher and DDSL) and Natalie Nicholson(DSL) are responsible for testing the filtering system on a weekly basis.
- Beth Weller (Safeguarding Governor) is responsible for testing the filtering system on a termly basis.

How to raise questions or concerns

Our filtering and monitoring system is designed to protect pupils online. It shouldn't have an impact on teaching and learning or school administration.

Contact **Lisa Crouch** if you and/or pupils:

- Cannot access content that you need to carry out your work

- Have access to content that should be blocked
- If you become aware of pupils accessing concerning content at any time, report this to **Natalie Nicholson** as soon as possible, if she is not available, please speak to any member of the DSL Team.