



DANE ROYD J&I SCHOOL

Online Safety Policy

Review frequency: Annually

**Approval by: Governing
Body**

**Date approved: 21st October
2026**

Policy date: October 2026

Review date: October 2027

Lead personnel: Mr Lee

Aims which guide our policies and practice at Dane Royd School



PERSEVERANCE

As a school, we aim to nurture an environment where children and staff achieve and thrive. We want to build strong foundations and a love of learning where every member of our school community feels they belong, can be, and become the very best version of themselves. We want our children to understand the rich heritage of the world; to be a positive member of their community and to become skilled citizens who have self-belief, passion and empathy for the world in which they live.

Our Agreed Strong Foundations are:



RESPECTFUL

- To create a school environment which nurtures and encourages a life-long love of learning.
- All members of the school community will live the school values. Through these values, we will equip our young people with the skills for life, to make them reflective, empathetic and open-minded members of the community.
- To provide vital enrichment activities to provide opportunities for our children to experience and thrive in.
- To teach the knowledge and skills to enable our young people to make informed decisions about their well-being, health and relationships to build their self-efficacy.
- To celebrate differences and diversity, and promote equity of opportunity so all can thrive together.
- To have high aspirations for all our young people. We want every child to succeed in their own way. Successful learning means enabling every individual – regardless of background, race, gender, disability, sexuality or socioeconomic status – to flourish in our school.
- To support pupils to become responsible, active citizens who can play their part in public life as young people and adults in modern Britain.
- We want our children and staff to be proud of their school. By following our school values, we will build a respectful, dynamic and inclusive school community where everyone's achievements are celebrated.



OPEN-MINDED



UNDERSTANDING



DETERMINED

We ensure that all of our policies and practices are guided by these aims and we seek to ensure that they are at the forefront of all that we do.

Table of Contents

Scope of the Online Safety Policy.....	4
Policy development, monitoring and review.....	4
Schedule for approval, monitoring and review.....	4
Policy and leadership.....	5
Responsibilities	5
Online Safety Group	8
Policy.....	9
Online Safety Policy	9
Acceptable use	10
Reporting and responding	14
Responding to Pupil Actions.....	17
Responding to Staff Actions.....	19
Use of Artificial Intelligence (AI)	19
Education.....	19
Online Safety Education Programme	19
Staff.....	20
Governors.....	21
External Stakeholders.....	21
Working with Parents and Carers	22
Wider Community and Agencies.....	22
Technology.....	23
Filtering and Monitoring.....	23
Technical Security.....	24
Cyber Security.....	24
Data Protection	24
Technology Practice.....	25
Device Management	25
Digital Content.....	26
Public Online Communications.....	26
Outcomes.....	27
Dane Royd Junior and Infant School's Online Safety Policy Appendices	29
A1 - KS2 Pupil Acceptable Use Agreement.....	30
A2 - Foundation and KS1 Acceptable Use Agreement.....	32
A3 Parent/Carer Acceptable Use Agreement.....	33
A4 Staff (and Volunteer) Acceptable Use Agreement.....	35
A5 Community Users Acceptable Use Agreement.....	38

Scope of the Online Safety Policy

This Online Safety Policy sets out how Dane Royd Junior and Infant School will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, pupils, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, Dane Royd Junior and Infant School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Policy development, monitoring and review

This policy has been developed by the Dane Royd's Online Safety Committee, drawing on the expertise and responsibilities across the school. Membership includes:

- Headteacher – Miss C Kelly
- Assistant Headteacher – Mr J Davison
- Online Safety Lead (OSL) – Mr M Lee
- Governors – Mrs C Midgley
- Parents/carers – PTA Members
- Digital Leaders – 6 children

Schedule for approval, monitoring and review

Approved by the Governing Body on: DATE

Monitored by: Miss C Kelly, Mr J Davison, Mr M Lee

Reporting to the Governing Body: Minimum termly via the Standards Committee

Policy review cycle: reviewed annually, or sooner in response to significant technological developments, emerging risks, or incidents.

Next planned review date: September 2027

Escalation following serious incidents: the school will inform relevant external agencies as appropriate including, but not limited to, Wakefield Social Care, LADO and Police.

Monitoring the impact of the policy

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents recording on CPOMs.
- Filtering and monitoring records via Senso.
- Reviews of the effectiveness of the filtering systems.
- Internal network activity monitoring data via Eduthing IT Support.
- Surveys/questionnaires (as appropriate) of: pupils, parents/carers and staff.

Policy and leadership

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and Senior Leaders – Miss C Kelly and Mr J Davison

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

Governors

Governors approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated).
- Ensure that children be taught about safeguarding, including in relation to online safety.
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard.

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governors.
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Participate in the Online Safety Group.

Governors also support parent/carers and community engagement in online safety.

Designated Safeguarding Leads (DSLs) – Miss C Kelly, Mrs G Kendall, Mrs B Ellam, Mr M Lee, Mrs C Ward

The DSLs will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- With the nominated SLT Lead and the IT provider lead the (at least annually) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.
- Report regularly to SLT and drive continuous improvement across relevant policies and practice.
- Ensure appropriate support for pupils with SEND.

Online Safety Lead (OSL) – Mr M Lee

The OSL will:

- Lead the Online Safety Group and support the DSLs day to day.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training.
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Lead – Mrs G Kendall

Curriculum leads will work with the DSLs/OSL to deliver a planned online safety programme. This will be provided through a discrete programme (2BeSafe), PSHE and RSE programmes, assemblies and pastoral programmes, and relevant national initiatives and opportunities such as Safer Internet Day and Anti-Bullying Week.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise pupil use of technology and follow procedures for online safety issues.
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider / technical staff - Eduthing

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.

- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSLs.
- Monitor systems for misuse and report concerns promptly to Miss C Kelly (Headteacher).
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Pupils

Pupils will:

- Follow the Pupil AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the pupil AUA.
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

Community users

Community users who access school systems / X feed and PTA Facebook group as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. The school welcomes partnership working and shares good practice where appropriate.

Online Safety Group

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice.

Membership

- Headteacher / DSL – Miss C Kelly
- OSL / DSL – Mr M Lee
- Senior Leader – Mr J Davison
- Senior Leader / Curriculum Lead / DSL – Mrs G Kendall
- Online Safety Governor - Mrs C Midgley
- IT/technical representative - Eduthing
- Digital Leaders
- Parent/carers representatives

Core responsibilities

The group supports the DSLs/OSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from pupils, staff and parents/carers and turn this into improvement actions.
- Promote pupil voice, peer support and awareness activity.
- Track and evidence improvement actions.

Governance and impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Pupil Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

Policy

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection policies.

What the policy does

- Defines responsibilities for online safety.

- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.
- Supports compliance with KCSIE, DfE Technical Standards and UK GDPR.
- Promotes pupils' digital competence and critical understanding.

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually and sooner if risks/technology change.
- Monitored by the DSLs/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity.
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to pupils and parents/carers through AUAs and awareness activity.
- Published on the school website.

Acceptable use

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs). AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement:

- staff and pupil induction/handbooks.
- posters in areas where technology is used.
- curriculum and awareness sessions.
- communications with parents/carers.
- school website.
- peer support.

Acceptable/Unacceptable Actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
material or comments that are:	- Encouraging, promoting or assisting suicide/self-harm - Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) - Incitement to, or threats of, violence - Hate crime - Public order offences (including harassment and stalking) - Drug-related offences - Weapons/firearms offences - Fraud and financial crime (including money laundering)					
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	- Misusing someone else's username/ID or password to access data, software or systems without authorisation - Gaining unauthorised access to school networks, data or files (including bypassing security controls) - Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) - Phishing, credential theft, or attempting to capture passwords or personal data - Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) - Disabling, impairing or disrupting network/services (e.g., denial of service) - Using penetration-testing tools without explicit permission					X
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

	Staff and other adults				Pupils			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (e.g. Roblox, Fortnite, Minecraft)			x				X	
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)			x		X			
Cloud storage and file sharing (e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents)		x			X			

Social media and user-generated platforms (e.g. <i>TikTok, Instagram, Snapchat, X, Reddit</i>) and other age-restricted services			x		X			
Messaging, chat and voice (e.g., <i>WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts</i>)			x		X			
Streaming entertainment/media (video, music, podcasts) e.g. <i>Netflix, Disney+, Spotify</i>			x		X			
Video platforms and livestreaming (e.g. <i>YouTube, Twitch, TikTok LIVE, Instagram Live</i>)			x		x			
Personal mobile phones and smart devices on site (phones, smartwatches, earbuds).		X			X			
Taking photos/video/audio on devices (including sharing, location data and consent)			x		X			
Other personal devices (e.g., <i>tablets, handheld consoles, VR headsets, wearables</i>)			x		X			
Personal email accounts on site or on the school network/Wi-Fi (e.g., <i>Gmail, Outlook.com</i>)			x		X			
School email used for personal communication (non-work/non-learning)	x				X			
Unapproved AI tools/services (<i>generative AI chatbots and image/video tools, AI companions, browser extensions</i>)	X				X			

Reporting and responding

Introduction

Dane Royd Junior and Infant School is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges (2021)*, which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child

Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSLs, OSL, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
 - Child sexual abuse material (CSAM).
 - Non-consensual or self-generated images.
 - Grooming, exploitation, or sexual harassment.
 - Terrorism or extremism.

- Hate crime, fraud, extortion, stalking.
- Cyber offences under the Computer Misuse Act.
- Sale of illegal substances or goods.
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

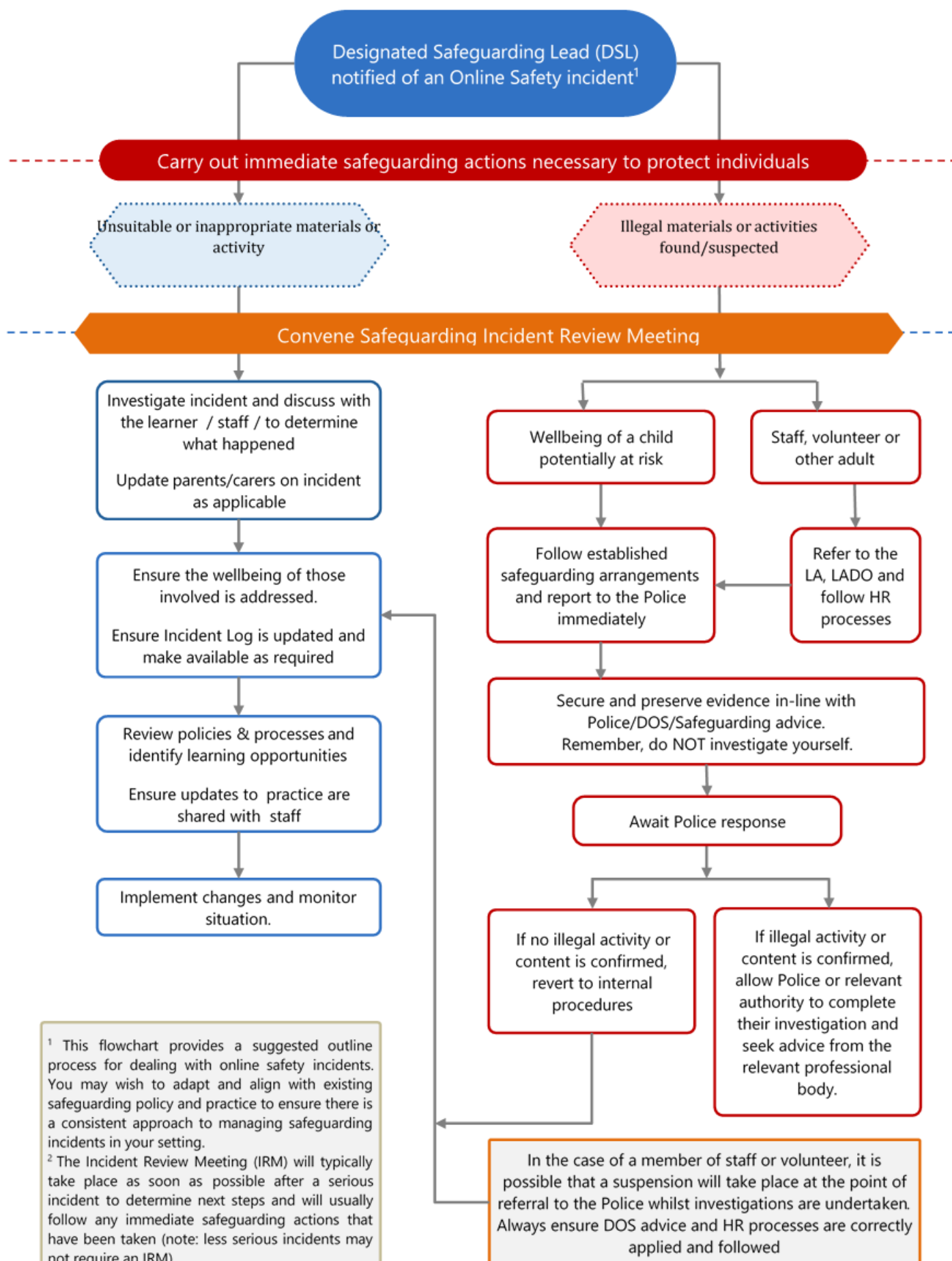
Recording and Monitoring

The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
 - The Online Safety Group.
 - Senior leaders.
 - Governors (via safeguarding reports).
 - *Staff.*
 - *Pupils, where appropriate.*
 - *Parents/carers through general communications.*
 - *Local safeguarding partners where relevant.*

The school will work with appropriate external agencies when required, including:

- Local Authority safeguarding teams.
- Local Authority Designated Officer (LADO).
- Police / CEOP.
- Local Safeguarding Partnership guidance.
- UK Safer Internet Centre's Professionals Online Safety Helpline.
- Reporting Harmful Content service.



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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Pupil Actions

Incidents	Refer to class teacher/tutor	Refer to DSL / OSL	Refer to SLT	Refer to Police/Social Services	Refer to IT Services Provider	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X	X	X	X	X	X
Unauthorised access to the school network , including using another person's account or sharing usernames/passwords.	X	X				X	X	X	X
Damaging, corrupting or deleting another user's data.	X	X			X	X	X	X	X
Sending offensive, harassing or bullying emails, texts or messages.	X	X			X	X	X	X	X
Unauthorised downloading/uploading , file sharing or distribution of files.	X	X			X	X	X	X	X
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).	X	X	X		X	X	X	X	X
Failing to report accidental access to offensive or pornographic material	X	X				X	X	X	X
Deliberately accessing offensive or pornographic material (or attempting to)	X	X	X	X	X	X	X	X	X
Sharing or receiving content that breaches copyright or data protection law.	X	X				X	X	X	X

Unauthorised use of devices , including taking photos/videos or audio recordings and using a smartphone in school.	X	X	X	X		X	X	X	X
Unauthorised use of online services (apps, websites or platforms).	X	X	X	X	X	X	X	X	X
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X	X	X	X	X	X	X	X	X
Repeated breaches of these rules following previous warnings or sanctions.	X	X	X	X	X	X	X	X	X

Responding to Staff Actions

The head teacher and HR manager will act in a proportionate manner on a case-by-case basis and will follow the LA agreed and adopted staff code of conduct which covers the inappropriate use of electronic equipment.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: pupil support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of pupils and staff remains central to our approach.

For more information on how and why AI is used at Dane Royd, please refer to our AI Policy.

Education

Online Safety Education Programme

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all pupils (2BeSafe), aligned to nationally recognised guidance and frameworks. Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship), with assessment and clear intended outcomes.

The programme develops pupils' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks.
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion.
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content.
- respect copyright and intellectual property, including when using online material and AI tools.
- understand and follow the pupil AUA, and act within moral and legal boundaries.

- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing.
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use.
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing.
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, pupils are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Pupil voice is actively used to strengthen the school's approach through feedback, pupil representation, and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities. Pupils are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

In line with [DfE Keeping Children Safe in Education \(KCSIE\)](#), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

All staff will receive online safety training and understand their responsibilities under this policy. Training will include:

- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Ensuring that staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported.
- Ensuring that staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement.
- Ensuring that staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles.
- Ensuring that staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for pupils are approved and managed.
- Ensuring that staff follow cyber security policy and requirements.

- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance.
- Support for staff knowledge-building.
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

Governors

Governors should take part in online safety training and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through:

- Attendance at training offered by the Local Authority or other relevant organisations (e.g. SWGfL).
- Participation in school training and information sessions. This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.
- Enhanced training will be provided for (at least) the Online Safety Governor. This will include:
 - Basic cyber security awareness training.
 - Training to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of pupils. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website and X.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving pupils in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources.
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches.
- accurate, balanced and age-appropriate information about changes affecting social media and other online services.
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place.
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement.

Wider Community and Agencies

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or X to offer online safety content suitable for the broader community.
- Drawing on the expertise of external agencies.
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice.

Technology

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., [DfE Technical Standards](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)) and best practice guidance (e.g., [UKSIC Appropriate Filtering and Monitoring](#)). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed.
- filtering blocks illegal content and provides age-appropriate and role-appropriate access.
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention.
- all school-owned devices are subject to filtering and monitoring.
- staff and pupils understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated.
- where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- where Generative AI products are used, they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products.
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content.

Oversight and Review

- Senior leaders, the Designated Safeguarding Leads (DSLs), technical staff and governors have clear roles and responsibilities.
- Governors 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 this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using [Testfiltering](#)). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding leads and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were

conducted; which devices and environments were tested, issues identified and actions taken.

- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central.

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions.
- devices, networks and systems are protected through secure configuration, patching and malware protection.
- backups and recovery arrangements are in place to reduce the impact of system failure or attack.
- incidents and weaknesses are reported, recorded and used to inform improvement.
- responsibilities for technical security are clearly defined and supported by appropriate expertise.
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents.

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats.
- senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance.
- staff and pupils are educated/trained to recognise and report cyber security concerns.
- business continuity and incident response arrangements are maintained and reviewed.
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation.

The school ensures that:

- personal data is processed lawfully, fairly and transparently.

- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place.
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests.
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely.
- data breaches are reported and managed in line with legal requirements.
- data protection is embedded across safeguarding, teaching, learning and administration.
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology.
- emerging safeguarding risks.
- national guidance and statutory expectations.

Technology Practice

Purpose

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in [Keeping Children Safe in Education](#), emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice, education and staff training. It also supports the DfE digital and technology standards and the school's responsibilities for filtering, monitoring, cyber security and digital leadership.

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education.

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated.
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies.
- appropriate technical and procedural controls are in place to support safe use.
- staff, pupils and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems.
- education on the safe and responsible use of devices forms part of the school's online safety education.
- pupils do not have access to mobile phones or other personal smart devices throughout the school day, in accordance with the school's Mobile Devices policies.
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons.
- staff model the school's requirements and use personal devices only where authorised and professionally appropriate.
- procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and current national guidance.

Decisions about device use are informed by risk assessment and reviewed regularly.

Digital Content

The school recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content.
- consent, privacy and safeguarding considerations are applied consistently.
- staff and pupils are trained/educated to understand their responsibilities when creating or sharing digital content.
- personal data and images are handled securely and lawfully.
- school-approved platforms and accounts are used where content includes personal or sensitive information.
- staff and pupils understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies.
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication.
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and

safeguarding risk from public platforms while reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse.

The school ensures that:

- public online communications are appropriate, accurate and well-managed.
- public communications from or regarding the school are monitored and addressed where appropriate.
- published content complies with safeguarding, data protection and statutory requirements.
- to reduce the risk of illegal manipulation of publicly available images of staff and pupils, the school has procedures in place to control how those images are shared online.
- publishing public communications is restricted to authorised and trained staff.
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts.
- staff understand expectations around professional conduct and online behaviour.
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour.
- emerging safeguarding risks.
- feedback from staff, pupils and parents.
- national guidance and statutory expectations.
- the school's progress towards meeting the DfE digital and technology standards.
- the impact of mobile-phone arrangements and changes affecting children's access to online services.

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, pupils and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes. Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.

- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety.

Dane Royd Junior and Infant School's Online Safety Policy

Appendices

A1 – KS2 Pupil Acceptable Use Agreement

A2 – Foundation/KS1 Pupil Acceptable Use Agreement

A3 - Parent/Carer Acceptable Use Agreement

A4 - Staff (and Volunteer) Acceptable Use Agreement

A5 - Community Users Acceptable Use Agreement

A1 - KS2 Pupil Acceptable Use Agreement

I agree to use the school's digital systems, devices and online services safely and responsibly to protect me, other pupils and the school.

Keeping Safe Online

- The school will check how I use devices and online services to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Devices and Online Services Sensibly

- I will only use devices, apps, games and websites that my teacher or parent/carer says are suitable for my age.
- I know that I am not allowed to use some online services and I know what they are.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I understand that not every app or website is suitable for children my age.
- If I want to join a new app, game or online community, I will speak to a trusted adult first.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.
- If I make a mistake online, I know I can ask a trusted adult for help.

What Happens If I Break These Rules?

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Pupil	
Group/Class	
Signed	
Date	

A2 - Foundation and KS1 Acceptable Use Agreement

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.
- I will only use apps and games that a trusted adult says are right for me.
- If I want to try a new game or app, I will ask a trusted adult first.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules?

- If I forget the rules, my teacher will help me learn to make better choices next time.

Signed (child): _____

A3 Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care. Parents are requested to sign the permission form overleaf to show their support of the school in this important aspect of the school's work.

As the parent/carer of the below pupil, I give permission for my son/daughter to have access to the digital technologies at school.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using devices.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of digital technologies at home and will inform the school if I have concerns over my child's online safety.

Name of Parent/Carer	
Name of Pupil	
Group/Class	
Signed	
Date	

A4 Staff (and Volunteer) Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible, informed and professionally competent users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that filtering and monitoring are safeguarding measures designed to protect pupils, staff and school systems. Where my role requires it, I will act promptly on concerns or alerts in accordance with the school's safeguarding procedures.
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school.
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any safeguarding, cyber security, filtering, monitoring or data protection concern using the school's agreed reporting procedures.
- I will complete the online safety, safeguarding and cyber security training required by the school and keep my knowledge up to date.

Protecting Pupils, School Systems and Information:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR).
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack.
- When using AI systems in my professional role, I will follow the rules set out in the AI school's AI policy.
- I will follow the school's expectations for the professional use of mobile phones and other connected devices, ensuring only permitted use.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will protect school systems by following the school's cyber security procedures.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will respect filtering, monitoring and other security measures and report any concerns about their effectiveness.
- I understand that some websites or services may be restricted for safeguarding reasons and will use the school's agreed process where access is required for legitimate educational purposes.

- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will only use school-approved cloud services and digital platforms for storing or sharing school information.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content.
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that my professional responsibilities extend to my conduct in public online spaces where this could affect pupils, colleagues or the reputation of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I will model safe, responsible and balanced use of digital technology in my professional practice.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Name	
Signed	
Date	

A5 Community Users Acceptable Use Agreement

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Signed	
Date	