RYDES HILL

PREPARATORY SCHOOL & NURSERY

Pupil E-Safety and Acceptable Use of Technology Policy

This policy also applies to EYFS

TABLE OF CONTENTS

Statement of intent

Rydes Hill understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Roles and responsibilities

The Governors will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Head of Rydes Hill's remit covers online safety.
- Approving this policy.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with IT staff and service providers.
- Ensuring that the SMT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Head of Rydes Hill ("the Head") is also the E-Safety Co-ordinator and will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Taking the lead responsibility for online safety in the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and IT.

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on an annual basis.

IT Support will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Head.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Be aware of the filtering and monitoring systems in place and will know how to escalate concerns where they are identified. Staff will be made aware of their expectations and responsibilities relating to filtering and monitoring systems during their induction.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Head has overall responsibility for the school's approach to online safety, with support from deputies where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The Head should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive updates regarding online safety information and changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online in Prep and in Senior external speakers are used to deliver information regarding online safety. Assemblies or small group sessions for Senior pupils will be provided where required on specific topics.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The Head will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the Head will balance the victim's wishes against their duty to protect the victim and other young people. The Head and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the Head decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Head, who decides on the best course of action in line with the relevant policies. If the concern is about the Head, it is reported to the Head of Tormead Prep or the Chair of Governors.

Concerns regarding a pupil's online behaviour are reported to the Head, who investigates concerns with relevant staff members, e.g. ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Head will contact the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity. The Head will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding Policy.

All online safety incidents and the school's response are recorded by the Head.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Parents are encouraged to inform the School immediately if they believe their child is being cyberbullied or there is an inappropriate use of IT.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Safeguarding Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are often unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child abuse imagery or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the Head without delay, who will manage the situation in line with the Safeguarding Policy.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil’s mental state, both positively and negatively. The Head will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The Head will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

The Head will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in IT lessons and PSHE.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

The Head will be involved with the development of the school's online safety curriculum. Relevant members of staff, e.g. the SENCO, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Head will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher should consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The Head will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Staff will use all smart technology and personal technology in line with the school's Staff IT and Electronic Devices Policy.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online. Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental newsletters to parents reinforce the importance of children being safe online and advise parents on appropriate online use, as well as its use in school.

Parents and carers will be made aware of what their children are being asked to do online when undertaking remote learning, including the sites they will asked to access and who from the School their child is going to be interacting with online.

Internet access

Staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Staff IT Acceptable Use Agreement.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

Governors will ensure the school's IT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. Governors will ensure ‘over blocking’ does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Head will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school’s safeguarding needs.

The School uses a Sophos filtering system. Weekly reports of flagged search terms are used to monitor internet usage and followed up by the Head. The Head regularly reviews the effectiveness of filtering and monitoring systems and includes this review in reports to the Governing Body.

The Head will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils’ ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system will be directed to the Head. Prior to making any changes to the filtering system, IT and the Head will conduct a risk assessment. Any changes made to the system will be recorded by IT. Reports of inappropriate websites or materials will be made to an IT immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the Head and IT, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school’s network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the Deputy Head Pastoral who will manage the situation

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. IT will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to IT.

All members of staff will have their own unique usernames and private passwords to access the school’s systems. Pupils in Reception and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum length and require a mixture of letters and numbers to ensure they are as secure as possible. Passwords do not expire, instead darkweb monitoring will alert us of any breached passwords, whereupon the user will be forced to change their password.

Users will inform IT if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Head will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to IT. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Any cyber-attacks initiated through emails will be managed in line with the Critical Incident Management Plan.

Use of devices including cameras

Staff members will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement. The School accepts no responsibility whatsoever for theft, loss or damage relating to mobile devices. It is the responsibility of parents and pupils to ensure mobile devices are safe and properly used.

Pupil's Ipads, Air Tags (and other tracking devices) and mobile phones are not allowed on visits, whether residential or day. School staff will carry a school mobile and will be able to communicate with the School Office and parents if needed. If pupils bring their phones to School they must be left with School Office.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) ‘Filtering and monitoring standards for schools and colleges’
- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2023) ‘Keeping children safe in education 2023’
- DfE (2023) ‘Teaching online safety in school’
- DfE (2022) ‘Searching, screening and confiscation’
- DfE (2023) ‘Generative artificial intelligence in education’
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’

This policy operates in conjunction with the following school policies:

- Technology Acceptable Use Agreement
- Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy