Online Safety Policy

Staff Responsible:	**Mr D Frankish**
Date of Issue:	September 2024
Review Date:	September 2025

Ribbon Academy Trust
Online Safety Policy

Contents

1. Introduction

The purpose of online safety at Ribbon is to:

- Educate pupils about online safety issues and appropriate behaviours, so that they remain safe and legalonline.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To minimize the risks of handling sensitive information.

Different technologies

This policy refers to the use of different technologies, these include:

- Computers, laptops, iPads, iMacs, iPods, and other hardware devices that have access to the internet
- Websites, emails, and applications

Effective Practice in online safety

Online safety depends upon effective practice in each of the following areas:

- Education for responsible IT use by staff and students.
- A comprehensive, agreed and implemented online safety Policy.
- Secure, filtered broadband.
- A school network that is compliant with National Education Network standards and specifications.

Links to relevant legislation and guidance: -

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 (2024) 'Keeping children safe in education 2024'
- 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'

Links to other policies:

- As noted in this policy, the school has Staff Code of Conduct and a separate Acceptable Use Policy for pupils.

- Links are also established with the school's Anti-Bullying Policy, Behaviour Policy, policies for Child Protection and Staff Code of Conduct.

Our online safety Policy has been written by the school, building on the Kent online safety Policy and NSPCC and government guidance. It has been agreed by senior management and approved by Directors.

- The online safety Policy was revised by Mr D Frankish (Online Safety Leader)

- The next review of this policy is scheduled for September 2025

2. Roles and responsibilities

The role of the Head teacher and Senior Leadership Team in online safety at Ribbon:

- The HT is responsible for ensuring the safety (including online safety) of members of the school community
- The HT will appoint a designated person as Online safety Leader for the school.
- The HT and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The HT and SLT are responsible for ensuring that the Online safety Leader and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The role of the Trustees in online safety at Ribbon:

- The Board of Trustees has a nominated link to Computing and IT and a nominated safeguarding Director, both of whom oversee policies and meet with key staff asneeded. Policies are reviewed by the Board of Trustees biannually.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT 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

The role of the DSL will be responsible for:

- Taking the lead responsibility for online safety in 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 ICT technicians.
- 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.
- 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.
- 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 a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

The role of the online safety leader at Ribbon (Mr Danny Frankish) is:

- To oversee the curriculum, ensuring all members of the online safety team are aware of their roles, responsibilities, and requirements to produce documentation.
- To ensure planning and resources are available for staff to deliver a progressive online safety curriculum, across the academic year.

- To ensure that all pupils and staff sign up-to-date policies.

The role of the IT Technician at Ribbon (Neil Williams) is:

- 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 headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

Teaching and Support Staff at Ribbon are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy andpractices
- they have read and understood the school Staff Code of Conduct a copy of which is available in on SharePoint > Documents > Policies
- they report any suspected misuse or problem using CPOMs
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and Acceptable Use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor IT activity in lessons, extra-curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras, smart watches, and handheld devices
- they monitor the use of devices listed above and implement current school policies about these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for theiruse and that processes are in place for dealing with any unsuitable material that is found in internet searches (as per Behaviour Policy)

Pupils:

- are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (please see Computing Curriculum Plans for more guidance)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials andknow how to do so (as per Safeguarding protocols and policy)
- will be expected to know and understand school policies on the use of mobile phones, digital cameras,smart watches, and handheld devices
- should know and understand school policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

- Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

- We, therefore, take every opportunity to help parents understand these issues through newsletters, parents' evenings, parents' afternoons & literature.

3. Staff training

All members of staff at Ribbon receive annual Safeguarding training. This specifically includes online safety training. Details of members of staff who have received training can be found from the school's Safeguarding team (Mrs D Richardson).

The DSL 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.

4. Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st-century life for education, business, and social interaction. At Ribbon, we have a duty to provide students with high-quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

- Ribbon's Internet access will be designed expressly for pupil use and will include filtering appropriateto the age of pupils. (Please see Filtering Policy).

- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils. (Please see Acceptable Use Agreement).

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation. (Please see online safety planning).

Pupils will be taught how to evaluate Internet content

- At Ribbon, we ensure that the use of Internet-derived materials by staff and by pupils complies with copyright law.

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

How online safety is covered in the curriculum

Children at Ribbon have access to a progressive online safety curriculum. Online safety is a part of everyday practice, although children do receive discrete safety lessons every year. Every classroom in KS1 displays the Acceptable Use Agreement, signed by children, alongside an online safety display, which teachers refer to during everyday teaching (see Section 7.1). Every classroom in KS2 displays the Acceptable Use Agreement, signed by children, alongside the Be Internet Legends key characteristics display, which teachers refer to during everyday teaching(see Section 7.1).

Pupils with SEND

Pupils with SEND have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties.

The school makes the following provisions to protect those children:

- Any SEND children with identified language, communication or social difficulties are identified on the school's SEND list. Teachers are aware of those children and differentiate online safety lessons as required.
- Children in Kaleidoscope Room have differentiated online safety lessons as part of their specialist provision.
- SEND children work with Sue Farrell from Place 2 Be and address issues during a Y6-Y7 transition groupduring the summer term in Y6.

5. Managing Internet Access

Information system security

At Ribbon, our information-system security is put in place, monitored, and overseen by Mr N Williams, the school's IT Technician.

- School IT system security will be reviewed regularly by Mr N Williams and the SLT.
- Virus protection is installed and updated regularly. Details of which can be obtained from Neil Williams.
- Security strategies are discussed with the Local Authority.

Email

At Ribbon, we use the Local Authority's email system, for staff and pupils (www.durhamlearning.net). Before using school emails (when the service is available from the Local Authority), children will sign an Acceptable UseAgreement, and take part in online safety lessons, to learn about possible dangers and how to keep safe online.

Students may only use approved e-mail accounts on the school system.

- Students must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others or arrange tomeet anyone without specific permission.
- Incoming e-mail should be treated as suspicious, and attachments not opened unless the author is known.
- Any emails to outside bodies, for the sake of research or learning by the children, are sent via theclass teacher, and approved by the Head teacher before sending.
- The forwarding of chain letters is not permitted.

Published content and the school website, app, Class Dojo and Facebook group

At Ribbon, we have a vast and informative website (www.ribbonacademy.org.uk). It includes up-to-date news and information about school. The site will be updated by Mr N Williams, with overall editorial responsibility taken by the Head Teacher, to ensure content is accurate and appropriate. Before content is added, the following rules should be considered, and adhered to:

- Staff or student personal contact information will not generally be published.
- The contact details given online are the school's main office.
- Children's full names will never be used on the school website.
- Children's names will never accompany a photograph.
- Pupils without published photograph permission will not appear.

Letters and term dates are published on Class Dojo and The Ribbon Facebook. Both can be downloaded via the App Store or via Google Play. Mrs N Ball (PA to Headteacher & Wider SLT) will be responsible for uploading content, although the overall editorial responsibility will be taken by the Head Teacher, who will ensure content is accurate and appropriate. Before content us added, the following rules should be considered, and adhered to:

- Staff or student personal contact information will not generally be published.
- The contact details given online are the school's main office.
- Children's full names will never be used on the school website.
- Children's names will never accompany a photograph.
- Pupils without published photograph permission will not appear.

To keep in touch with parents, the school also has an official Facebook group. It includes links to the school website, as well as news updates for parents. The DHT and administrative assistants will be responsible for uploading content to the page. Overall editorial responsibility will be taken by the Head Teacher, who will ensure content is accurate and appropriate. Before content is added, the following rules should be considered, and adhered to:

- Staff or student personal contact information will not be published.
- The contact details given online are the school's main office.
- Children's full names will never be used by the school.
- Children's photographs will only be uploaded if the school has written permission from parents. This is obtained from the GDPR agreement, completed by all parents when their children join the school.
- **Children <u>without</u> permission for photograph use are reported to class teachers each September and a list can be obtained at any time from the office.**
- During school trips, key members of staff are identified (in risk assessment) to capture key images. Parents are NOT permitted to capture images of the children.

Each class teacher also uses Class Dojo to contact parents and give updates about daily school life. Before content is added, the following rules should be considered, and adhered to:

- Staff or student personal contact information will not be published.
- Children's full names will never be used on Class Dojo.
- Children's names will never accompany a photograph.

Publishing students' images and work

- Photographs that include students will be selected carefully so that individual pupils cannot be identified, or their image misused.
- Children's names will never accompany a photograph.
- Written permission from parents or carers will be obtained before photographs of students are publishedon the school website or Class Dojo.
- Work can only be published with the permission of the student and parents/carers.

Social networking and personal publishing

- The school will control access to social networking sites and consider how to educate students in theirsafe use.
- Students will be advised never to give out personal details of any kind which may identify them, their friends, or their location. They will be advised of this during online safety lessons (see section 3.2.1).
- Students should be advised not to place personal photos on any social network space without consideringhow the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should be advised to only invite known friends and deny access to others.
- Students should be advised that advertising scams can be dangerous. This will be covered during e-safety lessons (see section 3.2.1).

Staff use of Social Networking

All staff at Ribbon are asked to sign a Code of Conduct agreement, which includes a section on responsible useof social media. These are kept by the Finance Department. A copy can be found on SharePoint > Documents >Policies

Managing filtering

- The school will work in partnership with Durham LEA, Becta and the Internet Service Provider to ensurethat systems to protect pupils are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the online safety Leader or the IT technician and a CPOM report completed.
- The ITSS technician will ensure that regular checks are made to ensure that the filtering methods selectedare appropriate, effective, and reasonable.

Managing videoconferencing

- Students should ask permission from the supervising teacher before making or answering a videoconference call, using Skype or Facetime.
- Videoconferencing will be appropriately supervised for the students' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- The online safety team understands that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. (Please see Filtering Policy)

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. (Please see Mobile Phone Policy – Section 13.1)

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.

6. Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct' before using any school IT resource at Ribbon.

- All children and staff in school have controlled, monitored access to the internet. If any AUPs are broken, and the Behaviour Policy deems them to have restricted internet access, ITSS and class teachers will actionthis.

- Parents/carers will be given a copy of the Acceptable Use Form, which their children have signed.

Assessing risks

- At Ribbon, we will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor DCC can accept liability for any material accessed, or any consequences of Internet access.

- The online safety leader (AT) will annually audit IT use to establish if the online safety policy is adequate and thatthe implementation of the online safety policy is appropriate and effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Management Team in accordance to the school's Behaviour Policy.

- Any complaint about staff misuse must be referred to the HT.

- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

- If parents or pupils have a complaint, they should follow the school's complaints procedure.

- Any potentially illegal issues will be dealt with by the SLT and police/parents.

7. Communicating online safety

Introducing the online safety policy to pupils

- online safety rules will be posted in all rooms where computers are used.
- Pupils will be informed that network and Internet use will be monitored.
- All children will sign a Key-Stage-Appropriate AUP.
- A programme of training in online safety will be developed, based on the materials from CEOP (seesection 6.)

Staff and the online safety policy

- All staff will be given the school online safety Policy and its importance explained.
- During online safety annual training, staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management andwork to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship. (See section 11.1)

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school online safety Policy in newsletters, the school brochure and on the school website.
- The school will maintain a list of online safety resources for parents/carers.

8. The misuse of technology and breaching the policy

All staff at Ribbon sign a Code of Conduct and children sign an Acceptable Use Agreement to raise awareness ofthe dangers of using technology incorrectly, as well as ensuring the safety of both staff and pupils.

Both agreements are set to last for the duration of their time at Ribbon. If agreements are broken, children face consequences appropriate to the action, which could range from a day's ban to a meeting with parents.

Teachers are responsible for ensuring that the children's rules are on display in every classroom, serving as a daily reminder for children of all ages.

How incidents are reported

As part of our Safeguarding policy, staff are required to record any concerns or incidents that have occurred to do with online safety. A CPOM alert must be filled in at the earliest opportunity. This procedure should also be followed ifchildren access a website deemed to be inappropriate for school use. ITSS will be informed to block the website using the school's internet filtering system. All staff are trained on using CPOMs and must report to D Richardson if theyneed another copy of their username and password. Any misuse of the internet, in accordance with the Acceptable Use Policy, should be dealt with following the school's Behaviour Policy.

9. Parental involvement

Parents can access the online safety policy on our school website.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. We, therefore, take every opportunity to help parents understand these issues through newsletters, parents' evenings, parents' afternoons & literature.

10. How images and film are managed

Details about how images and film of children are stored for, and for how long, are detailed in the school's Data Protection Policy.

11. Statement on passwords and password security

As part of the school's Code of Conduct and Acceptable Use Policies (for both staff and pupils), passwords shouldnot be shared and should be unique. If any members of staff have any concerns about passwords, they should complete a CPOM alert.

12. The use of mobile technologies including mobile phones

At Ribbon, children are not permitted to use their mobile phones in school. If a parent wishes for his/her child to bring a mobile phone to school (for use on the way home or for a young carer), the parent should contact school staff and discuss the issue first with their child's teacher. The phone must be handed in to the child's teacher first thing in the morning, who will place it in a locked cupboard, and it will remain switched off. It can then be collected by the child at home time (the phone is left at the owner's own risk). If, in the rare case of a Young Carer, for whom communication with home is essential, it should be done with prior consent by staff and parents and the use of the school telephone agreed.

13. Sanctions for the use of mobile phones during school time for children

Mobile phones brought into school without permission by children will be confiscated, put in a locked cupboard, and returned at the end of the day. Where mobile phones are used in or out of school to bully or intimidate others, then the Anti-Bullying Policy will be applied.

Incidents outside of school between children involving mobile phones

If arguments, cyberbullying or any other issues involving children and technology occur outside of school, and the issue is brought to our attention, the peer-relationship issue in school should be dealt with in line with the Anti- Bullying Policy. We will offer support and guidance to finding a solution. We will assure the child that it is not his or her fault; notify the child's parent(s) and word with the child/parent to identify the bully. We will agree a way parents and children can take action to get the bullying to stop. We will tell the parent/child to work together to document all incidents (including printing emails, taking screen shots of text messages, and writing down all incidents in a notebook). This documentation will help when going to the correct authorities on the bullying. We will also advise the child and parents to block the bully from social media sites so he/she cannot see or comment on the child's page. Similarly, blocking the bully's phone number on the child's phone and his/her email address inthe child's email account would be advised.

Until the situation is under control, we will ask parents to limit the child's access to the internet and mobile device. This will reduce the exposure that the bully has to the child and will prevent the child from feeling depressed over something that occurred online.

Any referrals to Place 2 Be will be made, as would be the case with any upset or issue.

Staff use of mobile phones in school

Staff mobile phones should be switched off and left in a safe place during lesson times. Staff should only use mobile phones in designated areas (staff room and classrooms if there are no children there). Staff should not send or receive texts in classrooms or use camera phones at any time. When taking photos of events in and out of school (including sporting events) staff should only use school equipment, without exception. Staff should never allow themselves to be photographed by pupils using anything other than school equipment. Staff should never contact students from their personal mobile phone or give their mobile phone number to students. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.

Parent use of mobile phones in school

To ensure full safeguarding of the children at Ribbon, parents / carers are not permitted to use mobile phones whilst on school property. Clear signs on display at the main entrance instruct parents / carers to switch off their mobile phones when entering the school. When hosting events, parents / carers will be reminded of this before the event begins.

Educational Visits and Outdoor Learning

When children are accessing learning in the extended school grounds, the local community or whilst on a school trip, the most senior member of the team will carry a mobile phone in case of an emergency. During this time, the device WILL NOT be used to make or receive personal calls or messages.

15) Filtering and monitoring online activity

The governing board will ensure the school's ICT 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'. The governing board 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 DSL 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 headteacher and ICT technicians 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. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

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

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, 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 DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.