Ribble Drive Primary School

Online Policy

RATIONALE

Safeguarding is a serious matter; at **Ribble Drive** we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

• To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

• To ensure risks are identified, assessed and mitigated (where possible) to reduce any foreseeability of harm to the student or liability to the school.

Thus, we will be enabled to realise both our Mission Statement:

"Be the Best You Can Be."

And our Disability Statement:

"To make all reasonable adjustments to ensure that any member of the school community with a disability is not placed at a disadvantage and to endeavour to anticipate their needs in advance of their participation in any activities within the school"

This policy applies to the **whole school**, including the EYFS

This policy supports Articles 3(Best Interests of the Child), 23 (Children with a Disability), 16 (Right to Privacy), 17 (Access to Information from the Media)and 31(Right to Leisure, Play and Culture): UNICEF: The Convention on the Rights of the Child.

ROLES AND RESPONSIBILITIES

Local Governing Body

The local governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Head Teacher regarding training, identified risks and any incidents.

Head Teacher

Reporting to the local governing body, the Head Teacher has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the online safety officer as indicated below.
The Head Teacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated online safety Officer has had appropriate CPD to undertake the day-to-day duties. All online safety incidents are dealt with promptly and appropriately.

Online safety Officer
The day-to-day duty of online safety officer is devolved to **Mr D Lord**
The online safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize himself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the Head Teacher.
- Advise the Head Teacher, governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or Technical Support.
- Make himself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher and responsible governor to decide on what reports may be appropriate for viewing.

Technical Support Staff
Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any online safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Head Teacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
- The IT System Administrator password is to be changed monthly.

All Staff
Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any online safety incident is reported to the online safety Officer (and an online safety Incident report is made), or in his/her absence to the Head Teacher. If you are unsure the matter is to be raised with the online safety Officer or the Head Teacher to make a decision.
- The reporting flowcharts contained within this online safety policy are fully understood.

All Students

The boundaries of use of COMPUTING equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of COMPUTING equipment or services will be dealt with in accordance with the Relationships and Behaviour policy.

Online safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children as such the school will ensure that parents have the skills and knowledge they need to ensure the online safety of children outside the school environment.

Through parents' evenings, school newsletters, Class Dojo and the school website, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student **Acceptable Use Policy** before any access can be granted to school Computing equipment or services.

Online Safety Committee

Chaired by the Governor responsible for Online Safety, the online safety Committee is responsible:

- to advise on changes to the online safety policy.
- to establish the effectiveness (or not) of online safety training and awareness in the school.
- to recommend further initiatives for online safety training and awareness at the school.

Established by the online safety Officer, responsible Governor and others as required, the online safety Committee will meet on a termly basis.

Technology

Ribble Drive Primary uses a range of devices including PC's, laptops, Apple devices. In order to safeguard the children and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – we use SOPHOS software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Coordinator, online safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher.

Email Filtering – we use SOPHOS software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted.

Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted:

- to staff upon signing this online safety and the staff Acceptable Use Policy;
- students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their first name and a two-figured number, e.g. john09@safeComputing.lincs.sch.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Ribble Drive Primary is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Ribble Drive Primary and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the online safety officer who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below)
- Class Dojo
- Seesaw

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are 'comment enabled', comments are to be set to 'moderated'.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license, which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource, which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online safety incident is to be brought to the immediate attention of the online safety Officer, or in his absence the Head Teacher. The online safety officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Ribble Drive Primary will have an annual programme of training, which is suitable to the audience.

Online safety for students is embedded into the curriculum; whenever Computing is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Once a year, the whole school participates in the national 'Safer Internet Day'.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The online safety officer is responsible for recommending a programme of training and awareness for the school year to the Head Teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the CPD Coordinator for further CPD.

Online Bullying

Online bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" – DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand online bullying and its effects.

A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how online bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's Relationships and Behaviour policy which must be communicated to all pupils, school staff and parents
- Gives Head Teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feel that an offence may have been committed they should seek assistance from the police.

- Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by online bullying.
- All incidents of online bullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of Online bullying.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to online bullying and the school's online safety ethos.

Sanctions for those involved in online bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive
- Other school sanctions for pupils and staff may also be used in accordance to the schools Anti-Bullying, Relationships and Behaviour Policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Prevent Training

As part of new legislation all staff in all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. This enables staff to be vigilant against radicalisation. As a result of this, staff will take level 1 prevent training on an annual basis. The completion of this course will be recorded and the certificate will be saved in the staff members CDP file.

Roles and Responsibilities of the Single Point of Contact (SPOC),

The SPOC for Ribble Drive Primary School is Mrs. J. Caunce (Head Teacher), who is responsible for:

- Ensuring that staff of the school are aware that you are the SPOC in relation to protecting students/pupils from radicalisation and involvement in terrorism.
- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.
- Raising awareness about the role and responsibilities of Ribble Drive Primary in relation to protecting students/pupils from radicalisation and involvement in terrorism.
- Monitoring the effect in practice of the school's RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.
- Acting as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.
- Collating relevant information from in relation to referrals of vulnerable students/ pupils into the Channel* process.
- Attending Channel* meetings as necessary and carrying out any actions as agreed.
- Reporting progress on actions to the Channel* coordinator.
- Sharing any relevant additional information in a timely manner.

*Channel is a multi-agency approach to provide support to individuals who are at risk of being drawn into terrorist related activity. It is led by the West Midlands Police Counter-Terrorism Unit, and it aims to

- Establish an effective multi-agency referral and intervention process to identify vulnerable individuals;
- Safeguard individuals who might be vulnerable to being radicalised, so that they are not at risk of being drawn into terrorist-related activity; and
- Provide early intervention to protect and divert people away from the risks they face and reduce vulnerability.

For pupils, the school will build pupils' resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Schools are already expected to promote the spiritual, moral, social and cultural development of pupils and, within this, fundamental British values. Personal, Social and Health Education (PSHE) can be an effective way of providing pupils with time to explore sensitive or controversial issues, and equipping them with the knowledge and skills to understand and manage difficult situations. The subject can be used to teach pupils to recognise and manage risk, make safer choices, and recognise when pressure from others threatens their personal safety and wellbeing. They can also develop effective ways of resisting pressures, including knowing when, where and how to get help. Schools can encourage pupils to develop positive character traits through PSHE, such as resilience, determination, self-esteem, and confidence.

Revised: Spring 2024
Review: Autumn 2026

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the online safety policy. Once you have read and understood both you must sign the policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the online safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to *Subject Access Requests under the Freedom of Information Act.*

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School COMPUTING - You are not permitted to use Computing equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal Computing - use of personal computing equipment is at the discretion of the Head Teacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the online safety officer.

Viruses and other malware - any virus outbreaks are to be reported to In4Tech and Bury IT as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Online safety– like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of computing whether you are with other members of staff or with students.

NAME :

SIGNATURE : **DATE**

:Acceptable Use Policy – Students Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school computing for schoolwork that the teacher has asked me to do.
I Promise – not to look for or show other people things that may be upsetting.
I Promise – to show respect for the work that other people have done.
I will not – use other people's work or Computing without permission to do so.
I will not – damage the computing equipment, if I accidentally damage something I will tell my teacher.
I will not – share my password with anybody. If I forget my password I will let my teacher know.
I will not – use other people's usernames or passwords.
I will not – share personal information online with anyone.
I will not – download anything from the Internet unless my teacher has asked me to.
I will – let my teacher know if anybody asks me for personal information.
I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.
I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
I understand – if I break the rules in this contract, there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date

Online safety Incident Log

Number:	Reported by:	Reported to:
	When:	When:
Incident Description: (What happened, involving which children and/or staff, what action was taken		
Review Date:		
Result of review:		

Signature (Head Teacher)		Date:	
Signature (Governor)		Date:	