

# Online Safety Policy

## 2024 - 2025



Person responsible for the Policy:	Headteacher and DSL
Approved by/date:	
Date Reviewed	November 2024
Date of Next Review	October 2025



### Contents

1. Aims 3  
2. Legislation and Guidance 3  
3. Roles and Responsibilities 3  
4. Educating Pupils about Online Safety 5  
5. Educating Parents and Carers about Online Safety 6  
6. Cyber-bullying 6  
7. Acceptable Use of the Internet in School 8  
8. Pupils using Mobile Devices in School 8  
9. Staff using Work Devices outside School 8  
10. How RLA will Respond to Issues of Misuse 9  
11. Training 9  
Appendix 1: EYFS acceptable use agreement (pupils and parents/carers). 11  
Appendix 4: Parents

and Carers acceptable use agreement 15

## **1. Aims**

RLA aims to:

- Have robust processes in place to ensure the online safety of all pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate our whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## **The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## **2. Legislation and Guidance**

This policy is based on DfE's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum Computing, Relationship Education and PSHE programmes of study and complies with our funding agreement and articles of association.

## **3. Roles and Responsibilities**

**3.1 The Governors** Our Governors have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. Our Safeguarding Governor will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by our DSL.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of ICT's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### **3.2 The Headteacher**

The Headteacher is responsible for ensuring that all staff understand this policy, and that it is being implemented consistently throughout RLA. The Headteacher receives regular Prevent reports detailing inappropriate access logs.

**3.3 The Designated Safeguarding Lead (DSL)** RLA's DSL and deputy roles are set out in our child protection and safeguarding policy and relevant job descriptions.

The DSL, supported by our ICT Lead, takes lead responsibility for online safe at RLA, in particular:

- Supporting the Headteacher in ensuring that all staff understand this policy and that it is being implemented consistently throughout RLA
  - Working with the Headteacher, ICT Lead and Manager and other staff, as necessary, to address any online safety issues or incidents
  - Managing all online safety issues and incidents in line with the school child protection policy
  - Ensuring that any online safety incidents are logged on CPOMS and dealt with in line with this policy
  - Ensuring that any incidents of cyberbullying are logged and dealt with in line with RLA's Behaviour Policy
  - Updating and delivering staff online safety CPD
  - Liaising with other agencies and/or external services if necessary
  - Providing regular reports on online safety in school to the Headteacher and/or governing board
- This list is not intended to be exhaustive.

### **3.4 The ICT Manager**

The ICT manager is responsible for:

- Putting in place appropriate levels of security protection measures through Blackpool Borough Council and locally enforced policies, e.g. filtering and monitoring systems, reviewed / updated regularly to assess effectiveness and ensure pupils are kept safe from potentially harmful, inappropriate content and contact online while at school, including terrorist and extremist material (Prevent Reporting)
- Ensuring that RLA's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring RLA's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and preventing downloading of potentially dangerous files
- Ensuring that users may only access the networks and devices through properly enforced password

protection

- Monitor Chromebook usage by children, carrying out regular spot checks
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

**3.5 All Staff and Volunteers.** All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and implementing this policy consistently
- Adhering to the terms on acceptable use of RLA's ICT systems and the internet and ensuring that pupils follow RLA's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on CPOMs with the ICT Lead alerted and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with RLA's Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

**3.6 Parents and Carers.** Parents and Carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of RLA's ICT systems and internet
- Parents/carers

can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent/carer resource sheet – [Childnet International](#)
- NSPCC website
- Thinkuknow

### **3.7 Visitors and Members of our Community**

Visitors and community members who use RLA's ICT systems or internet are made aware of this policy and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## **4. Educating Pupils about Online Safety**

Pupils will be taught about online safety as part of our Tiered Curriculum Offer - universal, targeted and specialist:

In addition to our own curriculum informed by the National Curriculum and SVT Skeleton, all schools have to teach: [Relationships and health education](#) in primary schools. At RLA this includes:

- being taught: what positive, healthy and respectful online relationships look like
- the effects of their online actions on others
- how to recognise and display respectful behaviour online

This complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (including online) whom they do not know
- How to evaluate what they see by making judgments about what they see online and not automatically assume that what they see is true, valid or acceptable e.g. looking for fake URL's and websites, explaining the risks of 'too good to be true' online offers, advertising and fake product sale
- Understand how targeted advertising and clickbait on searches and social media feeds is done through monitoring online behaviour
- How to recognise techniques used to persuade or manipulate others e.g. through misinformation, disinformation and hoaxes
- Identify and understand the consequences of fraud, scams and phishing
- Understand how online platforms and search engines gather personal data through 'harvesting' and 'farming', how they can protect themselves and the importance of acting quickly if something goes wrong.

Understand the risks of sharing personal information

- Understand and recognise what acceptable and unacceptable online behaviour looks like, including the importance of respect and empathy towards others
- Know that not everyone is who they say they are online and how to look out for fake profiles
- Understand why passwords are important, how to create secure passwords and how to keep them safe
- Understand that some online behaviours are abusive, extremist and can become illegal (e.g. sexting) and can incite violence; realising the implications of these including the implications for the victims
- How to identify online risks to be able to make informed decisions about how to act with consequences of actions in mind and the positive and negative aspects of their online reputation / digital footprint
- Know how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent on and offline.
- How to find information about privacy settings on various sites, apps, devices and platforms and

understand the limitations of these

- Know different strategies for staying safe when communicating with others, especially people they don't know or have never meet
- How to make informed choices in relation to the Online Media Strategy (<https://www.gov.uk/government/publications/online-media-literacy-strategy>)?? e.g. sharing personal data, online actions having offline consequences and understanding the risks of engaging with others
- How to navigate the internet and manage information (<https://www.gov.uk/government/publications/education-for-a-connected-world>) e.g. copyright and ownership and privacy and security
- Understanding age verifications and how this content may be damaging to under-age users; what age of digital consent means in relation to sharing information (minimum age of 13)?
- How content can be used and shared, how this may affect future prospects and how difficult it is to remove something once online
- How the persuasive design of apps and games encourage users to play longer and the importance of restricting time on devices???
- Know the risks of live streaming and understand that online behaviours should mirror offline behaviours
- How and when to seek safe ways of support when they have concerns online including identifying a trusted adult, accessing support from school, police (including CEOP), Childline, IWF and reporting content and contact through various platforms and apps

RLA's age and developmentally appropriate teaching underpins the knowledge and behaviours that help children navigate the online world safely and confidently regardless of the device, platform or app. This teaching is:

- built into existing lessons across the curriculum
- covered within specific online safety lessons
- covered using school-wide approaches including all aspects of school life – culture, ethos, environment and home-school partnerships

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for specific needs and for pupils with SEND.

## **5. Educating Parents and Carers about Online Safety**

RLA will raise parent and carer awareness of internet safety and emerging issues through Dojo; workshops; assemblies and in information via our website and social feeds. This policy will be shared with parents and carers and we will let parents and carers know:

- What systems RLA uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from RLA their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these can be raised with the class teacher or DSL. Parents/carers are also made aware of external avenues of reporting concerns such as CEOP, Childline, Police and Children's Social Care

Concerns, comments or queries about this policy can be raised with any member of staff, including the Headteacher.

## **6. Cyber-bullying**

### **6.1 Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also our Behaviour Policy.)

### **6.2 Preventing and Addressing Cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so within a support environment, including where they are a witness rather than the victim.

Staff actively discuss cyber-bullying with pupils, explaining reasons why it occurs, forms it may take and what the impact can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including personal, social, health and economic (PSHE) education and computing, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and will be dealt with in a timely manner. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### **6.3 Examining electronic devices**

The Headteacher, and any senior leader authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified at RLA as being a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised senior leader will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Having liaised with our DSL and Police, authorised senior leaders may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they

believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the leader should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL and Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through RLA's Complaints procedure.

## **7. Acceptable Use of the Internet in School**

All pupils, parents, carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of RLA's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to RLA's terms on acceptable use if relevant.

RLA's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.



We will monitor websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 5.

### **8. Pupils using Mobile Devices in School**

Authorised use of mobile devices to support the welfare and well-being of pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with RLA's Behaviour policy, which may result in the confiscation of their device.

### **9. Staff using Work Devices outside School**

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate RLA's terms of acceptable use. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from our ICT Manager.

### **10. How RLA will Respond to Issues of Misuse**

Where a pupil misuses RLA's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses RLA's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with our Staff Disciplinary Procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Headteacher and DSL will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

### **11. Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude or semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
  - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff develop better awareness to assist in spotting the signs and symptoms of online abuse, including the ability to ensure pupils can recognise dangers and risks in online activity; and can weigh up the risks; and develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and child protection policy.

## Appendix 1: EYFS Acceptable Use Agreement (pupils and parents/carers)

Dear Nursery and Reception Parents/ Carers,

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful learning tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and effective learning. We expect all children to be safe and responsible when using these digital technologies.

Please read and discuss these online safety rules with your child and return the slip below **to your child's class teacher**. If you have any concerns, or would like more information, please contact your child's class teacher.

Please display the Safe, Acceptable-Use Agreement in an ideal place to remind your child of our 'rules', co-produced by staff and our pupil leaders. Thank you.

.....

We have discussed this and ..... (Child's name) agrees to follow the rules outlined in the Acceptable Use Agreement and to support the safe, responsible use of ICT at RLA.

Parent / Carer Signature ..... Class ..... Date .....

### Our Safe, Acceptable-Use Agreement for Nursery and Reception Pupils



## Nurturing excellence through happy, confident self-aware learners

### Appendix 2: KS1 acceptable use agreement (pupils and parents/carers)

**Dear Year 1 and Year 2 (KS1) Parents/ Carers,**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful learning tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and effective learning. We expect all children to be safe and responsible when using these digital technologies.

Please read and discuss these online safety rules with your child and return the slip below to your child's class teacher. If you have any concerns, or would like more information, please contact your child's class teacher.

Please display the Safe, Acceptable-Use Agreement in an ideal place to remind your child of our 'rules', co-produced by staff and our pupil leaders. Thank you.

.....

**We have discussed this and ..... (Child's name) agrees to follow the rules outlined in the Acceptable Use Agreement and to support the safe, responsible use of ICT at RLA.**

**Parent / Carer Signature ..... Class ..... Date .....**

### Our Safe, Acceptable-Use Agreement for KS1 Pupils



**This is how we keep ourselves safe when we use computers and other digital technology:**

- I will ask a teacher or suitable adult if I want to use a computer, tablet or camera.
- I will only open the activities that a teacher or suitable adult has allowed me to use.
- I will take care of the digital technologies which I use, at home and in school.
- I will ask for help from a teacher or suitable adult if I am not sure what to do, or if I think I have done something wrong.
- I know that I must tell a teacher or suitable adult if I see something on screen that upsets me, makes me scared or that I am unsure of.
- I will keep my passwords safe and will never use someone else's.
- I know that personal information, such as my name, address and birthday should never be shared online.
- I know I must never communicate with strangers.
- I am always polite when posting on communication tools such as ClassDojo or Purple Mash.
- I understand that to keep myself and others safe, content is filtered and the websites I visit and the keywords I type are monitored.
- I understand that devices I use are regularly checked and if I break the rules I might not be allowed to use a computing device.

**Nurturing excellence through happy, confident self-aware learners**

### Appendix 3: KS2 acceptable use agreement (pupils and parents/carers)

**Dear Year 3, Year 4, Year 5 and Year 6 Parents/ Carers,**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful learning tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and effective learning. We expect all children to be safe and responsible when using these digital technologies.

Please read and discuss these online safety rules with your child and return the slip below to your child's class teacher. If you have any concerns, or would like more information, please contact your child's class teacher.

Please display the Safe, Acceptable-Use Agreement in an ideal place to remind your child of our 'rules', co-produced by staff and our pupil leaders. Thank you.

.....

**We have discussed this and ..... (Child's name) agrees to follow the rules outlined in the Acceptable Use Agreement and to support the safe, responsible use of ICT at RLA.**

**Parent / Carer Signature ..... Class ..... Date .....**

## **Our Safe, Acceptable-Use Agreement for KS2 Pupils**



**This is how we stay safe when we use computers and other digital technology:**

- I will only access digital technologies when a trusted adult has given me permission to do so and supervises me.
- I will respect the computing technology and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will only open and delete my own files. I will not open nor delete other people's files.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and passwords secure; this includes not sharing it with others.
- I will always use my own username and password to access RLA's network and online services such as ClassDojo, TTRock Stars, Purple Mash or email.
- I will use all communication tools such as email, blogs or messaging safely, respectfully and responsibly. I will only send messages that are polite and sensible. I will notify an adult immediately if I notice someone messaging who is not approved by the teacher.
- I will only use my own RLA e-mail address when e-mailing. I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not deliberately look for, save or send anything that could make others upset or scared. If I accidentally find anything like this, I will tell my teacher or parent immediately.
- I understand what personal information is. I will never share my own or other's personal information such as phone number, home address or names. I will not arrange to meet someone unless this is part of an approved RLA project, approved by my teacher, and a responsible adult comes with me.
- I will support RLA's approach to online safety. I will not deliberately upload or add any images, video, sounds or text that could upset any member of the RLA community.
- In order to keep myself and others safe, I know that RLA checks my files and the online sites I visit.

- I understand that there is monitoring in place (such as Smoothwall, firewalls and filtering) to keep myself and others safe. These filter content and monitor the websites I visit, the keywords I type and the files I download / upload to my device, both at home and at school.
- I understand that regular monitoring of devices is carried out and if I behave inappropriately whilst

**Nurturing excellence through happy, confident self-aware learners**

## Our Safe, Acceptable-Use Agreement for Parents and Carers



### Background and Purpose

With access to discover and learn rich dynamic content; global connectivity; a platform for creativity and a place to engage in collaboration, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely and responsibly access and use digital technologies, whilst being fully aware of how to protect and safeguard themselves.

Our Parent/Carer Safe, Acceptable-Use Agreement is intended to help share the importance that we place on keeping children safe, particularly in regard to online safety. We want to encourage and support parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and timely reporting.

RLA wants to provide every child with the best access it can to safe online technologies. We use firewalls, filtering, device restrictions and Smoothwall to ensure we provide a safe and secure online environment by filtering content and monitoring websites visited, keywords typed and files uploaded / downloaded. Alert systems ensure issues are flagged immediately, logged and key members of staff alerted to help protect children from unnecessary risks. Monitoring takes place on devices both in school and on RLA devices taken home. Our IT Manager also carries out regular spot check monitoring on devices used in school.

At RLA, we actively encourage children to think critically about content and communication to and from others; and to develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, RLA expects the children to demonstrate that they are responsible users of digital technologies at all times.

### Parents/Carers, we ask you to support us by:

- ✓ Sharing safe, responsible online behaviours with your child, emphasising the importance of our Safe, Acceptable-Use Agreement and its rules which your child has agreed to.
- ✓ Highlighting the importance of accessing only age appropriate content and sites
- ✓ Explain the pitfalls and potential inaccuracies of social media eg biased websites.
- ✓ Explaining how to keep an appropriate digital profile for your child.
- ✓ Discussing what is and what is not appropriate to share online.
- ✓ Emphasising never to meet anyone online; nor trust that everyone has good intentions.
- ✓ Reporting any concerns that you may have whether home or school based.
- ✓ Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- ✓ Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- ✓ Avoiding posting or replying to any comments about RLA to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

### Permission Access. By signing below, you are:

- ✓ agreeing to allow your child access to RLA's approved internet, ICT systems and educational services;
- ✓ aware that your child has signed/agreed to RLA's Safe, Acceptable-Use Agreement for RLA pupils;
- ✓ aware of your role and responsibility in keeping your child safe on-line

✂ —————

We have discussed this and ..... (child's name) agrees to follow the rules outlined in RLA's Safe, Acceptable-Use Agreement and to the safe, responsible use of ICT at RLA.

I .....(Parent/Carer's name) agree to model and supervise safe and

responsible digital behaviours at home.

Parent / Carer Signature ..... Class ..... Date .....

✂ — — — — —

## Nurturing excellence through happy, confident self-aware learners



## Safe, Acceptable-Use Agreement for RLA Staff



### Background and Purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for teaching, learning and assessment. Digital technologies give staff opportunities to enhance children's learning and enable staff to become more efficient and effective in their work. The very nature of digital technologies means that they should be used with care; particular attention must be given to demonstrate and model appropriate behaviours and avoidance of misuse at all times.

Professional integrity and strong moral purpose must be upheld at all times by all staff. It is the duty of all RLA staff to ensure that RLA children get the very best start to the world of digital technology, including providing a robust, rich online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Staff must develop children's critical thinking, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.

RLA's internet, network and ICT systems and service subscriptions must be used with the utmost professionalism at all times. RLA provides its staff with secure systems through firewalls, filtering, device restrictions and Smoothwall which have inbuilt filtering, monitoring and virus protection. Anyone with access to these systems should be aware that their use of the systems is monitored on RLA devices both in and out of school and this can be used to form evidence should any suspected infringements occur.

**By signing this agreement, you will have access to RLA's systems and technologies. You acknowledge that you agree to all the statements below; and that you have read and understand school policies which have a bearing on this agreement.**

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care;
- I will educate children in my care about the safe, responsible use of digital technologies, acting on any online safety issues in accordance with RLA's policies;
- I understand my use of RLA's ICT systems/networks/ technologies and internet are monitored through various technologies such as firewalls, filtering and Smoothwall
- I know that, in and out of RLA, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to RLA or impact on my role within RLA and wider community;
- I know what the GDPR is and how this has a bearing on how I access, share, store and create data;
- Any data that I have access to away from RLA must be kept secure and used with specific purpose. As outlined in RLA's Data Protection policy, it is my responsibility to ensure that, when accessing data remotely, I take every precaution to ensure the integrity and security of the data is maintained;
- I understand that I am fully responsible for my behaviours, in and out of RLA. As such, I recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role;
- I recognise that my social media activity (as noted in RLA's Staff Code of Conduct) can have a damaging impact on RLA and children in my care, if I fail to uphold my professional integrity at all times whilst using it;
- If I am contributing to RLA's social media account(s) or website(s), I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded;
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant educational reason to do so; and that permission has been granted by the Headteacher in writing for each occurrence;
- I will inform RLA at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about other's behaviour/conduct, I will notify the Headteacher at the earliest opportunity;
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause or incite harm, fear or upset to others;

- I will never download or install software for non-education purposes;
- I shall keep all usernames and passwords safe and never share them;
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely;
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the Headteacher.
- I understand that personal mobile devices shall not be used during times of contact with children. These devices will have password protection;
- I know that I am responsible for the appropriate use of personal technologies, such as smart watches, when working with children;
- Any educational visits or activities that require a mobile phone/ camera will be provided by RLA and any data collected on them will be used in accordance with RLA policies.

Staff Name.....

Signature ..... Date .....

**Nurturing excellence through happy, confident self-aware learners**