Ryelands Primary and Nursery School

Online Safety Policy and Practices

This policy was developed as part of a consultation process involving pupils, staff, parents and Governors of the school, based on best practice advice (where available) from Lancashire County Council.

The implementation of this policy will be monitored by the Senior Leadership Team and Governing Body.

This policy should be read in conjunction with the following documents:

- Teaching and Learning Policy
- Curriculum Policy
- EYFS Policy
- Computing Policy
- Child Protection Policy
- Health and Safety Policy

Policy Created:	October 2019	
First Presented to Governors for approval:	30th October 2019 (Curriculum Committee)	
Proposed Review Cycle/Next Date:	Annually	October 2022

Approved by (Headteacher) **Date:**	**Approved by (Governor)** **Date:**

Policy Review History		
Date: October 2020	**Date:** October 2021	**Date:**
Key Changes: - Reference to the remote learning policy	Key Changes: • Date only • Changed name: Stephenson to Barrett	Key Changes:
Presented to Governors: Curriculum Committee 11th November 2020	**Presented to Governors:** Curriculum Committee 10th November 2021	**Presented to Governors:**

Contents

1. Policy Aims

This Online Safety Policy has been written for Ryelands Primary School and is based on guidance from the Kent County Council Online Safety Policy (2019) and The Education People's Online Safety Guidance Document (September 2019). It also takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' 2019, 'Teaching Online Safety in School' 2019, 'Working Together to Safeguard Children' 2018.

At Ryelands School, we identify that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk.

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

The purpose of this Online Safety Policy is to

- safeguard and promote the welfare of all members of the Ryelands School community online.
- identify approaches to educate and raise awareness of online safety throughout our community.
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- identify clear procedures to follow when responding to online safety concerns.

2. Ryelands School Vision for Online Safety

We place a high value on the use of modern and emerging technologies, not only to augment effective teaching with a range of inspirational and engaging approaches, but as an essential training platform for young people who will needs specific ICT aptitudes and skills for a successful life, both personally and as members of the labour market. Effective use of ICT should enhance learning but also nurture creativity and technological thinking across the curriculum.

We recognise that online safety is an essential part of safeguarding and acknowledge its duty to ensure that all pupils and staff are protected from potential harm online.

This will be achieved by;

- providing a diverse, balanced and relevant approach to the use of technology
- encouraging children to maximise the benefits and opportunities that technology has to offer
- ensuring that children learn in an environment where security measures are balanced appropriately with the need to learn effectively
- ensuring children are equipped with the skills and knowledge to use technology appropriately and responsibly

- teaching children and their families how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- communicating to all users in our school community why there is a need for an Online Safety Policy, and a need to teach Online Safety.

2.1 Links with other policies and practices

This policy links with several other Ryelands School policies, practices and action plans, including but not limited to:

- Remote Learning and Action Plan
- Anti-bullying Policy (within the Behaviour Policy)
- Acceptable Uses of Technology Policies (AUP)
- Behaviour Policy (Including Anti Bullying Policy)
- Safeguarding and Child Protection Policy
- Whistleblowing Policy
- Confidentiality Policy
- Computing Policy
- Personal Social and Health Education and Citizenship Policy
- Relationships and Sex Education Policy
- Data Protection Policy
- Nurture Class Policy
- Early Years Foundation Stage Policy
- Teaching and Learning Policy

3. Monitoring and Review

Ryelands School will undertake the following:

- As technology evolves and changes rapidly we will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical and staffing infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

All members of staff in school, and members of the wider community, are expected to take responsibility for maintaining the safety of young people through a duty of care, and this includes safe and appropriate use of technology. However, in addition to this, the school has appointed an Online Safety Team to oversee and monitor the effective implementation of this policy.

The Designated Safeguarding Lead (DSL), Kelly Barrett, is recognised as holding overall lead responsibility for online safety. The ultimate lead responsibility for safeguarding and child protection, including online safety, remains with them.

In conjunction with the DSL, the Computing Subject Leader (CSL), Megan Garlick, will take responsibility for the teaching and learning of Online Safety within school and the wider community.

Both the DSL and CSL will work closely with the School Governors and the Senior Leadership Team (SLT) in order to ensure the Online Safety of the school.

4.1 The Senior Leadership Team will:

- Create a whole setting culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with Tech Hub North West LTD (refer sub sections 4.5 and 6.2 below) to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and the Computing Subject Leader by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all pupils to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Maintain records of online safety concerns, as well as actions taken, as part of the Ryelands School safeguarding recording mechanism (CPOMs).
- Ensure a coordinated approach across relevant safeguarding areas with other safeguarding leads.
- Take operational joint responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Take operational joint responsibility for ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Take operational joint responsibility for ensuring that all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Keep personally up to date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

- Provide or arrange Online Safety advice/training for staff, parents/carers and governors.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and Ryelands School's policies and procedures.

4.3 The Computing Subject Leader will:

- Take operational joint responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including AUPs.
- Take operational joint responsibility for ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Take operational joint responsibility for ensuring that all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Keep personally up to date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as CEOP.
- Provide or arrange Online Safety advice/training for staff, parents/carers and governors.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).

4.4 It is the responsibility of all Ryelands School members of staff to:

- Read and adhere to our Online Safety Policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with pupils
- Maintain a professional level of conduct in their personal use of technology, both on and off school site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care.
- Identify online safety concerns and take appropriate action by following the Ryelands School safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.5 It is the responsibility of staff managing Ryelands' technical environment (Tech Hub North West LTD) to:

- Ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

4.6 It is the responsibility of Ryelands School pupils (at a level that is appropriate to their individual age and ability) to:

- Engage in age/ability appropriate online safety education.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.7 It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the acceptable use of technology policies.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter online issues.
- Use our systems, such as Parent Pay, the Ryelands School Facebook page, the school website and Connect by Parent Apps, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

The three main areas of Online Safety risk (as mentioned by OFSTED, 2013) that school must be aware of and consider are:

Area of Risk	Example of Risk
Content:	- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence

Children need to be taught that not all content is appropriate or from a reliable source.	associated with often racist language), substance abuse. - Lifestyle websites, for example proanorexia/ self-harm/suicide sites. - Hate sites. - Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	- Grooming - Online bullying in all forms - Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	- Privacy issues, including disclosure of personal information, digital footprint and online reputation - Health and well-being - amount of time spent online (internet or gaming). - Sexting (sending and receiving of personally intimate images). - Copyright (little care or consideration for intellectual property and ownership – such as music and film).

5.1 Education and engagement with pupils:

Ryelands School will establish and embed a whole school culture of staying safe online. It will raise awareness and promote safe and responsible internet use amongst pupils by:

- ensuring our curriculum and whole school approach is developed in line with the DfE 'Teaching online safety in school' guidance.
- ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study- specifically the *Kidsafe* programme of study.
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
- creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
- involving the CSL, when required, as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content.
- making informed decisions to ensure that any educational resources used are appropriate for our pupils.
- using external visitors, where appropriate, to complement and support our internal online safety education approaches. The school will use the document *'Using External Visitors to*

  Support Online Safety Education: Guidance for Educational Settings' when considering these external visitors.
- providing online safety education as part of the transition programme towards the start of the academic year and across the key stages and/or when moving between establishments.
- rewarding and celebrating positive use of technology.
- differentiating learning about online safety learning in order to ensure that all pupils access this vital learning
- displaying safe use information in all rooms with internet access.
- informing pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
- consulting with the CSL about how to mark whole school events, such as Online Safety Week, in school.

Ryelands School will ensure that all pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age appropriate education regarding safe and responsible use precedes internet access.
- teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- enabling them to understand what acceptable and unacceptable online behaviour looks like.
- preparing them to identify possible online risks and make informed decisions about how to act and respond.
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Pupils

- Ryelands School recognises that any pupil can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- Ryelands School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable pupils.

5.3 Training and engagement with staff

Ryelands School will

- ○ ensure that all staff, upon starting work at the school, are required to agree to the school's AUP and are provided with a copy of the Online Safety Policy and key staff guidelines, which includes personal safeguarding.
- ○ provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. All training and advice will be delivered by the Online Safety Team, specifically the CSL

- Staff training covers the potential risks posed to pupils (content, contact and conduct) as well as our professional practice expectations.
- make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with pupils.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.
- ensure that all staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting Online Safety whilst using ICT

5.4 Awareness and engagement with parents and carers

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Ryelands School offers regular opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies. This takes place through:

- School newsletters
- A dedicated area on the school website, which promotes external Online Safety resources and online materials.
- Parents Online Safety Awareness sessions and advice available from the Online Safety Team

5.5 Informing and engagement with Governors

Governors are kept updated on arising Online Safety matters through the Annual Report to Governors for ICT and Online Safety. Governors also review and agree the Online Safety Policy annually, following discussion with the Online Safety Team.

5.6 Acceptable Use Policy (AUP)

An AUP is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. This agreement is a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of pupils who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.
The school has the following AUPs in place (see appendices):

Computing AUP – Staff and Governor Agreement

Computing AUP – Supply Teacher and Visitors/Guests Agreement
Computing AUP – Pupils Agreement/Online Safety Golden Guidelines
Computing AUP – Parent's AUP
Computing AUP – Wi-Fi

6. Ensuring the Safer Use of Technology

6.1 Guidelines for the safer use of technology

In Ryelands School the following statements outline what we consider to be pupil guidelines for the safer use of technology:

- Absolutely no abusive or disrespectful language will be allowed at any time.
- Students are not allowed to share their passwords or log in under someone else's name.
- In 'discussions', negative comments towards another user will not be tolerated. It is ok to disagree about topics, but this must not become personal.
- Any student who views something they are not happy with should tell an adult.
- If you click on a page you are unsure of by accident, close it immediately and tell a trusted adult.
- Never give out personal information – address, telephone numbers etc.
- It is very important that students understand that **all** actions occurring Virtual Learning Environments (VLE's) are observable by the administrator of the site. Even when a post is deleted by a student, it is saved by the application and therefore can be accessed by the administrator at any time.
- Consequences of rule infractions will be determined by the Headteacher in line with Ryelands Behaviour Policy.

6.2 Technical Support:

Ryelands School network is managed Tech Hub (North West) Ltd. through a service level agreement and they are responsible for all aspects of network technical support and maintenance. They also visit the school once a week to perform maintenance and solve any issues.
The following procedures are to be followed to ensure the network and all data remains secure:

- The safety and security of the network is reviewed by Tech Hub (North West) Ltd. on each maintenance visit.
- Tech Hub (North West) Ltd. ensure that all computers are configured to receive all necessary updates and patches.
- If any users suspect a breach of network security, they should inform the CSL immediately. The CSL will then contact Tech Hub (North West) Ltd. for assistance.
- The Online Safety Policy is devised in consultation with Tech Hub (North West) Ltd. who are aware of all requirements and standards regarding Online Safety.
- The Ccsland members of the Senior Leadership Team are responsible for liaising with and managing the technical support staff from Tech Hub (North West) Ltd. when using school computers. Handovers are made after each visit to ensure essential maintenance has taken place.

6.3 Software:

- All software used in school must be owned by the school, or by staff at the school, with appropriate user licenses used.
- Software is installed on systems by Tech Hub (North West) Ltd. The school has a central resource of software titles and should any more be needed members of staff are asked to make a request to the CSL for purchase at whole school level.

6.4 Classroom use

- Ryelands School uses a wide range of technology. This includes access to:
  - Computers, laptops, iPads, iPods
  - The Internet, including search engines and educational websites
  - Multiple educational apps
  - Email
  - Digital cameras and in-built PC webcams
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use appropriate search tools as identified following an informed risk assessment of the types of things students will be searching on the specific search engine. Our pupils are briefed preceding every search-engine opportunity to come away from an upsetting search result and immediately tell a member of staff.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to pupils age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils age and ability.
  - **Key Stage 2**
    - Pupils will use age-appropriate search engines and online tools.
    - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils age and ability.

6.5 Managing internet access

- All staff, Governors, pupils and visitors will read and agree an AUP before being given access to our computer system, IT resources or the internet on our school network.

6.6 Filtering and monitoring

6.6.1 Filtering managed through technical services

- Ryelands' Online Safety Team, in conjunction with Tech Hub North West LTD have ensured that our school has age and ability appropriate filtering and monitoring in place to limit pupil's exposure to online risks.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience
- The Online Safety Team, in conjunction with Tech Hub North West LTD, will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The Online Safety Team are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

6.6.2 Appropriate filtering

- Ryelands School's education broadband connectivity is provided through BT Internet
- Ryelands School uses BT Internet Netsweeper
    - BT Internet Netsweeper blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
- We work with BT Internet to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If pupils or staff discover unsuitable sites or material, they are required to turn off monitor/screen and report the concern immediately to a member of staff, report the Uniform Resource Locator (URL) of the site to Tech Hub North West LTD
- Filtering breaches will be reported to the DSL (or CSL) and technical staff and will be recorded and escalated as appropriate.
- Where necessary to safeguard a child's wellbeing, parents/carers will be informed of filtering breaches involving pupils.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or Child Exploitation and Online Protection Centre (CEOP).

6.6.3 Appropriate monitoring

- Where a specific concern exists, we will appropriately monitor internet use on all setting owned or provided internet enabled devices.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via monitoring approaches, we will record the incident via the CPOMS referral system, after the standard systems of child safeguarding referral have been followed (see attached flowchart)

6.7 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our **Confidentiality Policy**

6.8 Data security and management of information systems

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire ICT Security Framework (published 2005) has been consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school. In line with the requirements of the General Data Protection Regulation (GDPR 2018) sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

In Ryelands School, data is kept secure and all staff are informed as to what they can/cannot do regarding data in the following ways:

- Key information is held on the school's Server accessed through password protection.
- Members of staff are given access permissions based on their role and levels of responsibility in school.
- The Headteacher has ultimate responsibility for managing access to different levels of information for all employees and young people in school.
- As part of the Induction process for new staff or procedures for staff changing roles individuals are updated on the location of data specifically required for their role.
- Induction also confirms the sensitive and confidential nature of all data held.
- Any data taken form the school environment is held on password protected school owned and maintained laptops, and/ or encrypted external hard drives.
- All staff are required to read, sign and return the school's Acceptable Use Policy (AUP).
- Staff understand that they should only use approved means to access, store and dispose of confidential data.
- Staff who remotely access school data understand the dangers of unsecured wireless access at home.
- We recommend that staff password protect their own mobile devices.

We take additional steps to ensure the security of our information systems, including:

- (Sophos) Virus protection being updated regularly and being present on all appropriate school devices.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all users on our school network from Year 3.
- **All** users are expected to log off or lock their screens/devices if systems are unattended.

6.8.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 3, all pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system.
    - follow a platforms guidance for frequency of password alteration on systems such as CPOMS and our school email intranet
    - not share passwords or login information with others or leave passwords/login details where others can find them.
    - not to login as another user at any time.
    - lock access to devices/systems when not in use.

6.9 Managing the safety of Ryelands School website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or pupil's personal information will not be published on our website; the contact details on the website (and given out in any format and setting) will be our setting address, email and telephone number.
- The administrator account, and teacher editing accounts, for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

6.9.1 Guidelines for the acceptable use of our School website:

- The school website will be maintained and updated by the School Admin Team or other appropriate staff.
- The website is a fundamental place for communicating Online Safety messages to pupils and parents/carers and has a dedicated Online Safety section.
- All staff are aware of the guidance for the use of digital media and personal information on the website.
- Any material for the website is passed to the School Admin Team, who updates the website periodically, ensuring relevant guidance is adhered to.
- Staff may add suitable educational content too their class blog page, ensuring relevant guidance is adhered to.
- All materials on the website shall adhere to copyright restrictions.
- Sensitive documents should only be available in 'read-only' formats, such as PDFs.

6.10 School email systems

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, Acceptable Use of Technology Policies and the Behaviour Policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider where appropriate.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- The CPOMS referral system is for recording wellbeing and pastoral issues. This system will be managed by Phase Leaders and the Pupil Support Team, including the DSL.

6.10.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, and are discouraged from communicating after 6pm.

6.10.2 Pupil email

- KS2 pupils may use a provided email account for educational purposes.
- Pupils will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

6.11 Use of digital media (cameras and recording devices)

The use of cameras and sound recording devices offer substantial benefits to education but equally present school with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites. Photographs and videos of children and adults may be considered as personal data in terms of General Data Protection Regulation (GDPR 2018).

6.11.1 Photo and video consent and purpose

- Each year school asks parents to complete an Image Consent Form. These are collated and permissions communicated to class teachers and club leaders in school. This consent includes the purpose, storage and media use of images. Each class' consent forms are included in an essential information folder in all classrooms. Children without image consent wear yellow lanyards during school events in order to ensure the fulfilment of the Image Consent Form.
- Where children are Looked After by the Local Authority, Image Consent Forms will also be required for the child's social worker
- The consent of adult staff members to have their photographs taken is assumed.
- The purpose of any photography is always communicated to those involved (e.g. assessment, display, celebration, website, media).
- Consent forms include permission to store images. Further consent will be sought if the school intends to use a photograph after a pupil has left.

6.11.2 Staff taking photographs / video

- All adults in school are permitted to take photographs for school purposes at the direction of class teachers using school owned equipment.
- If a child does not want to be photographed their choice will be respected. Children are not filmed or photographed when this might cause embarrassment, distress or if the child is injured.
- In addition, photography that could be misinterpreted is also avoided e.g. close up shots of children participating in PE activities.
- Teachers will take a range of photographs representing many or all class members.
- Group shots, with a background context are favoured.
- Photos will only be taken by staff on school devices, never on staff's personal devices

6.11.3 Parents taking photographs/ video

Under the GDPR parents are entitled to take photographs of their own children on the provision that the images are for their own use, e.g. at a school production. At these events parents are reminded that images and video **cannot** be published on social networking sites.

6.11.4 Storage of photographs / video

- All images are stored of password protected school equipment. On rare occasions images may be taken of site for the purposes of producing a display; in these instances, they are kept on the same password protected equipment and returned to school.
- Staff do not store images on personal equipment.

- Access to equipment containing images is managed and monitored by class teachers. All computer users in school are expected to log off or lock their devices if systems are left unattended. It is also the class teachers' responsibility to delete and dispose of digital and printed video/images.
- Emailed images are sent within the school's secure email system.
- Full names of pupils are never published with images.

6.11.5 The media, 3rd parties and copyright

When in school 3rd parties are supervised at all times. If 3rd parties wish to take photographs or videos it is understood that the consent of the parents of subjects must be obtained (see Image Consent Form). In this instance the copyright for these images passes to the 3rd party. It is understood that the modification, copying and redistribution rights of these images passes to the third party.

6.12 Educational use of webcams

- Ryelands School recognise that the use of webcams can bring a wide range of learning benefits.
- Approval must be sought in advance from the Headteacher prior to any educationally motivated videoconferencing taking place.
- Only secure, approved programs to be used for video conferencing.
- All pupils will be supervised when using video conferencing.
- It should be made clear to the receiver that no recordings may be taken without permission.
- Staff know how to terminate the video conference at any time.
- All webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Staff will ensure that external videoconferencing opportunities and tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

6.12.1 Users

- Videoconferencing will be supervised appropriately, according to the pupils age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- The unique log on and password details for any videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

6.12.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the pupils.

6.13 Management of applications (apps) used to record children's progress

We use Seesaw and our school website to record our pupils' learning and share appropriate information with parents and carers.

- The Online Safety Team will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard pupil's data
    - only school devices, on the secure school network, will be used for apps that record and store pupils' personal details, attainment or photographs.
    - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

7. Social Media

7.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of the Ryelands School community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of the Ryelands School community are expected to engage in social media in a positive and responsible manner.
    - All members of the Ryelands School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control pupil and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school hours for personal use is permitted for staff in the staff room only.
    - The use of social media during school hours for personal use is not permitted for pupils.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary action.
    - Members of the Senior Leadership Team may update the school Facebook page; however, they must not leave the Facebook account logged in on their personal devices, and they must keep the password secure.
- Concerns regarding the online conduct of any member of the Ryelands School community on social media, will be reported to the DSL or Headteacher and be managed in accordance with our anti-bullying, whistleblowing, allegations against staff, behaviour and child protection policies.

7.2 Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction.
- Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our Acceptable Use Policy.
- If a Social Network site is used by staff, details must not be shared with pupils and privacy settings be set at maximum. Staff should be aware that 'friends of friends' may be able to view 'tagged' photographs/comments, which may bring the individual member of staff or the school into disrepute. Comments made and photographs posted reflect the professional reputation of the school, and once posted cannot be un-done.

7.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
    - Disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Ryelands School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- Governors are encouraged not to identify themselves as Governors of Ryelands School on their personal social networking accounts; this is to prevent information being linked with the setting.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

7.2.2 Communicating with pupils and parents/carers

- Staff will not use personal social media accounts to contact pupils or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the headteacher in each individual circumstance.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard pupils, the setting and members of staff.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use official setting provided communication tools (email, visits to the school).
- Any communication from pupils and parents received on personal social media accounts will not be responded to on that platform and will be recorded via the CPOMS referral system.

7.3 Pupils' personal use of social media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we do not support the personal use of social media platforms by our pupils, unless they fall within the recommended age guidance, and can use the platform safely.
- Any concerns regarding pupils use of social media will be dealt with in accordance with existing policies, including safeguarding, anti-bullying and behaviour.
- Concerns regarding pupils use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Pupils will be advised:
    - to constantly be aware of the risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords.
    - to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.
    - how to report concerns on social media, both within the setting and externally.

7.4 Official use of social media

- Ryelands School official social media channels are:
    - Facebook: https://www.facebook.com/Lancaster-Ryelands-Primary-and-Nursery-School-335514539884446/
    - Twitter: https://twitter.com/ryelandsps

    - The official use of social media sites by Ryelands School only takes place with clear educational or community engagement objectives and with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - Official social media sites are suitably protected and, where possible, linked to our website.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Any official social media activity involving pupils will be risk assessed and heavily supervised by staff.

7.4.1 Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Be aware they are an ambassador for the setting.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure appropriate consent has been given before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any private/direct messaging with current or past pupils or parents/carers.
    - Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

8. Mobile Technology: Use of Personal Devices and Mobile Phones

- Ryelands School recognises that personal communication through mobile technologies is part of everyday life for many pupils, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

8.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of the Ryelands School community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of the Ryelands School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of the Ryelands School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

8.2 Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy such as confidentiality, safeguarding and acceptable use of technology.
- Staff will be advised to
    - keep mobile phones and personal devices in a safe and secure place lesson time.
    - only use personal devices in the staff room
    - keep mobile phones and personal devices switched off or switched to ‘silent’ mode during lesson times.
    - ensure that Bluetooth or other forms of communication, such as ‘airdrop’, are hidden or disabled during lesson times.
    - not use personal devices during teaching periods, unless permission has been given by the Headteacher in emergency circumstances.
    - ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Staff are encouraged to appropriately use their mobile phone as a safety control measure during school trips- only when necessary.

- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.

    - Any pre-existing relationships which could undermine this, will be discussed with the Headteacher
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - directly with pupils and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, disciplinary action may be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted.

8.3 Pupil use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - Ryelands School expects pupils' personal devices and mobile phones not to be brought into school.
    - Where it is deemed as necessary from a perspective of safety by the parents/carers of a child, pupils may bring their mobile devices into school. Before the school day, their switched off devices must be handed in to the school office, where they will be stored until collection at the end of the school day.
    - Pupils, parents and carers are aware that the school takes no legal responsibility for the safekeeping of pupils' personal devices.

- If parents/carers need to be contacted in the case of an emergency on behalf of a pupil, staff will accommodate and supervise the contact
    - Parents are advised to contact their child via the school office.
- Mobile phones or personal devices will not be used by pupils during the school day.
- Mobile phones and personal devices must not be taken into examinations.
    - Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a pupil breaches this requirement, the phone or device will be confiscated and held in a secure place.
    - Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our Behaviour Policy.
    - Pupils mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
    - Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the school day.

- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

8.4 Visitors' use of personal devices and mobile phones

- Visitors, including Governors, volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or CSL) or Headteacher of any breaches of this policy.

8.5 Officially provided devices and mobile devices

- Ryelands School staff laptops and iPads will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Ryelands School staff laptops and iPads will always be used in accordance with the acceptable use of technology policy.

9. Responding to Online Safety Incidents

See reporting concerns flowchart (see contents) for guidelines and procedure for reporting concerns about child and/ or staff online safety.

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including online bullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- We require staff, parents, carers and pupils to work in partnership with us to resolve online safety issues.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL or CSL will seek appropriate, expert advice- whilst remaining in line with our school Confidentiality Policy
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

9.1 Concerns about pupil online behaviour and/or welfare

- The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our Safeguarding and Child Protection Policy.
- All concerns about pupils will be recorded in line with our Child Protection Policy.

- Ryelands School recognises that whilst risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- Appropriate sanctions and/or pastoral/welfare support will be offered to pupils as appropriate, in line with our Behaviour Policy.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10. Procedures for Responding to Specific Online Concerns

If an Online Safety incident occurs, that contravenes the Online Safety Policy or agreed AUP's, it is important the protocol below will be followed. It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged via the CPOMS referral system.

10.1 Indecent Images of Children (IIOC)

- Ryelands Primary School will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software (provided by BT Internet Education Services)
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our Safeguarding and Child Protection Policy and the relevant procedures.
    - immediately inform appropriate organisations, such as the police.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation (IWF) via www.iwf.org.uk .
    - ensure that any copies that exist of the image, for example in emails, are deleted.
    - report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on Ryelands School provided devices, we will:

- ensure that the Headteacher is informed in line with our Whistleblowing Policy.
- the Headteacher or DSL will inform the relevant organisations including the LADO (Local Authority Designated Officer), in accordance with our managing allegations against staff policy.
- quarantine any devices until police advice has been sought.

10.2 Online bullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Ryelands School
- Full details of how we will respond to cyberbullying are set out in our Behaviour Policy (Including Anti-Bullying).

10.3 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Ryelands School and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (CSL) will obtain advice through the Education Safeguarding Service and/or the police.

10.4 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site, via enlisting the use of BT Internet Education Services' filtering system
- If we are concerned that a pupil or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Child Protection Policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with our Child Protection Policy/Whistle-Blowing Policy.

10.5 Online Sexual Violence and Sexual Harassment between Children

- Key staff at Ryelands School have accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- At Ryelands School we recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding and Child Protection Policy and Anti-Bullying Policy.
- We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Staff at Ryelands School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Personal, Social and Health Education (PSHE) and Relationships and Sex Education (RSE) curriculum, for example through Kidsafe.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on pupils electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate consequences in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL will discuss this with Lancaster Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

10.6 Youth Produced Sexual Imagery ("Sexting")

- Ryelands School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding Staff at Ryelands School will ensure that all members of the community are made aware of the

potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods, for example Kidsafe.

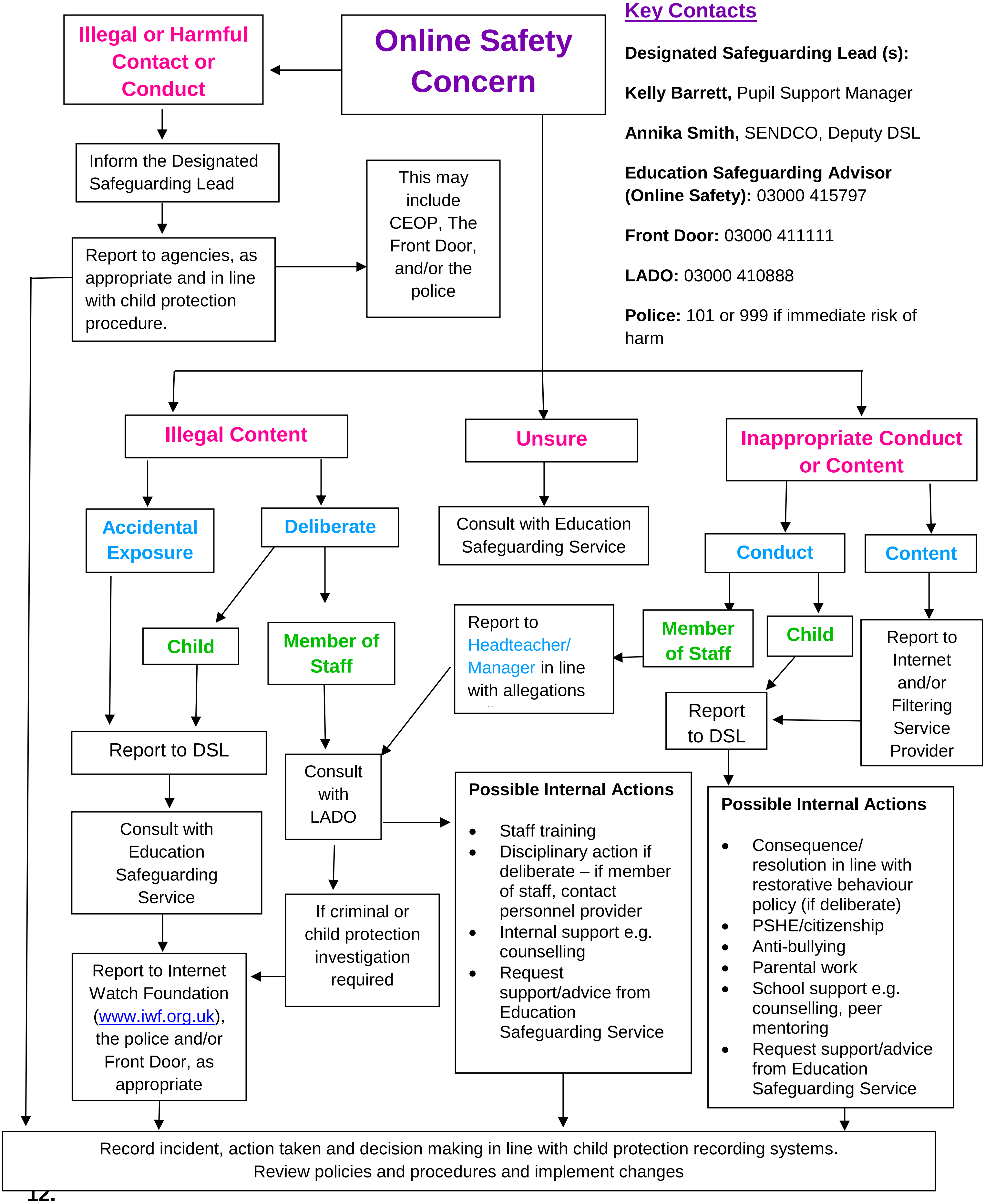
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policy Lancashire Safeguarding Children Board (LSCB) procedures.
    - Ensure the DSL responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Children's Social Care and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate consequences in accordance with our behaviour policy but taking care not to further traumatise victims.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

10.7 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Ryelands School will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- At Ryelands School we recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy CSL?).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
    - We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to pupils and other members of our community on our school website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Child Protection Policy and Lancashire Safeguarding Children Board (LSCB) procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/appropriate) and immediately inform Lancaster police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Service and/or Lancashire Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If pupils at other setting are believed to have been targeted, the DSL (or deputy CSL?) will seek support from Lancashire Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

11.

Responding to an Online Safety Concern Flowchart



Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate and in line with child protection procedure.

This may include CEOP, The Front Door, and/or the police

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

Report to Internet Watch Foundation (www.iwf.org.uk), the police and/or Front Door, as appropriate

Consult with LADO

If criminal or child protection investigation required

Unsure

Consult with Education Safeguarding Service

Report to Headteacher/ Manager in line with allegations

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling
- Request support/advice from Education Safeguarding Service

Inappropriate Conduct or Content

Conduct

Content

Member of Staff

Child

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions

- Consequence/ resolution in line with restorative behaviour policy (if deliberate)
- PSHE/citizenship
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

Record incident, action taken and decision making in line with child protection recording systems. Review policies and procedures and implement changes

Key Contacts

Designated Safeguarding Lead (s):

Kelly Barrett, Pupil Support Manager

Annika Smith, SENDCO, Deputy DSL

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm

12.

Links and Resources for the Ryelands School community:

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org

Appendix 1:

ICT Acceptable Use Policy (AUP):
Children
Early Years and Key Stage 1 (0-6)

Ryelands Primary and Nursery School

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

1. **I only ever use the internet when an adult is with me**
2. **I only click on links and buttons online when I know what they do**
3. **I keep my personal information and passwords secret and safe**
4. **I only send messages online which are polite and friendly**
5. **I know that my school can see what I am doing when online at school**
6. **I always tell an adult, teacher or member of staff if something online makes me feel unhappy or worried**
7. **I never meet anybody who I have met online**
8. **I will not bring any of my own devices into school**
9. **I can visit www.thinkuknow.co.uk to learn more about keeping safe online**
10. **I have read and talked about these rules with my parents/carers**

I have read the above AUP. I agree to support my child in following the Online Safety rules and to support the safe use of ICT at Ryelands Primary School.

Parent /Carer Name (Print) …………………………………………………………………………………………….

Parent /Carer (Signature) ……………………………………………………………………. …………………………..

Class ………………………………………………… Date…………………………………………………………………….

EYFS and Key Stage 1 Golden Guidelines

I only go online with a grown up

I am kind online

I keep information about me safe online

I tell a grown up if something online makes me unhappy or worried

APPENDIX 2

Ryelands Primary and Nursery School

ICT Acceptable Use Policy (AUP): Children Key Stage 2 (7-11)

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

Safe

- I only send messages which are polite and friendly.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission.
- I only talk with and open messages from people I know, and I only click on links if I know they are safe.
- I will only communicate online with people a trusted adult has approved.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my school has approved of.
- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I keep my personal information, and that of others, safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information on Pupil Share.
- I will only open/delete my own files at my teacher's request.
- I will only change the settings on the computer if a staff member has allowed me to.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school iPads and computers, and internet access, will be monitored.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then steps may be taken in line with Ryelands' behaviour policy.

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I always talk to a trusted adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.

- If I see anything online that I shouldn’t or that makes me feel worried or upset, then I will minimise the page and tell an adult straight away.

*If you feel your child is not able to understand this agreement, please contact the SENDCO for an alternative.

Ryelands Primary School Acceptable Use of Technology Policy – KS2 Pupil Agreement

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when:

1. I use school systems and devices, both on and offsite.
2. I use my own equipment out of the Ryelands School community, in a way that is related to me being a member of the school community, including communicating with other pupils of the school or accessing the school website or social media.

Name……………………………………………… Signed…………………………………………………….

Class…………………………………… Date……………………….

Parent/Carers Name………………………………………………....

Parent/Carers Signature…………………………………………….

Date………………………………………………………………………

Key Stage 2 Golden Guidelines

I ask a trusted adult about which websites I can use

I will not assume information online is true

I know there are laws that stop me copying online content

I know I must only open online messages that are safe. If I’m unsure I won’t open it without speaking to an adult first

I know that people online are strangers and they may not always be who they say they are

If someone online suggests meeting up, I will always talk to an adult straight away

I will not use technology to be unkind to people

I will keep information about me and my passwords private

I always talk to a trusted adult if I see something which makes me feel worried

APPENDIX 3

ICT Acceptable Use Policy (AUP): Children SEND

Ryelands Primary and Nursery School

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

1. I ask a grown up if I want to use the computer
2. I make good choices on the computer
3. I use kind words on the internet
4. If I see anything that I don't like online, I tell a grown up

We have discussed this Acceptable Use Policy and my child _______________________________ agrees to follow the Online Safety rules and to support the safe use of ICT at Ryelands Primary School.

Parent /Carer Name (Print) …………………………………………………………………………………………………….

Parent /Carer (Signature) ……………………………………………………………………………. …………………………..

Class ……………………………………………………. Date…………………………………………………………………….

APPENDIX 4

Ryelands Primary and Nursery School

Ryelands Primary and Nursery School
Torrisholme Road
Lancaster
LA1 2RJ

Telephone: 01524 64626
E-mail: admin@ryelands.lancs.sch.uk
Website: www.ryelands.lancs.sch.uk

Headteacher: Mrs Linda Pye

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all pupils, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate.

This is particularly relevant when using Social Media Sites that incorporate age-restriction policies. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

Pupils should not bring devices, including mobile phones, into school. If you insist that your child requires a mobile phone, please contact the Headteacher to discuss the matter further.

The enclosed ICT Acceptable Use Policy forms part of the wider School Online Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing Online Safety as part of your child's learning, we will also be holding Parental Online Safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about Online Safety for parents and carers, please visit the Lancsngfl e-Safety website;

http://www.lancsngfl.ac.uk/Online Safety

Yours sincerely,

Miss Megan Garlick
Computing Subject Leader

APPENDIX 5

Ryelands Primary and Nursery School

Ryelands Primary and Nursery School
Torrisholme Road
Lancaster
LA1 2RJ

Telephone: 01524 64626
E-mail: admin@ryelands.lancs.sch.uk
Website: www.ryelands.lancs.sch.uk

Headteacher: Mrs Linda Pye

Image Consent Form

Name of the child's parent/carer: ____

Name of child: ____

Year group: ____

Please read the Conditions of Use on the back of this form then answer questions below. The completed form (one for each child) should be returned to school as soon as possible.

	Yes	No
1. Do you agree to photographs/videos of your child being taken by authorised staff within the school?		
2. Do you agree to photographs/videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra-curricular events?		
3. May we use your child's image in printed school publications and for digital display purposes within school?		
4. May we use your child's image on our school's online publications e.g. website / blog / VLE?		
5. May we record your child on video?		
6. May we allow your child to appear in the media as part of school's involvement in an event?		

I have read and understand the conditions of use attached to this form

Parent/Carer's signature: __________________________________

Name (PRINT): __________________________________

Date: __________________________________

Conditions of Use

1. This form is valid for this academic year 2019/ 2020.
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.
8. Images/videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.

2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).

3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

APPENDIX 6

Ryelands Primary and Nursery School

Ryelands Primary and Nursery School
Torrisholme Road
Lancaster
LA1 2RJ

Telephone: 01524 64626
E-mail: admin@ryelands.lancs.sch.uk
Website: www.ryelands.lancs.sch.uk

Headteacher: Mrs Linda Pye

Consent Form for Images to be Taken e.g. at a School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in our school production / event name on <insert date/s>. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place regarding taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images/video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

Should any parents / carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.

These decisions are not taken lightly, but we must consider the safeguarding of all our children and respect parents' rights to privacy.

*This letter will only be used when necessary. For most performances in school, it will not be required.

Yours sincerely,

Headteacher

Child's name: ________________________________ Date: ____________________________

I agree / do not agree to photographs / videos being taken by third parties at the <insert event> on

<Insert date /s>.

Signed ______________________________________ (Parent / Carer)

Print name __________________________________

APPENDIX 7

ICT Acceptable Use Policy (AUP) - Staff and Governors

Ryelands Primary and Nursery School

ICT and the related technologies are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Media Platforms, Forums and Chat rooms.
5. I will follow the Online Safety Policy's guidance on connecting with pupils, parents and past pupils on social media platforms.
6. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
7. I will respect copyright and intellectual property rights.
8. I will ensure that all electronic communications with children and other adults are appropriate.
9. I will not use the school system(s) for personal use during working hours.
10. I will not install any hardware or software without the prior permission of Megan Garlick (Computing Subject Leader)
11. I will not use any of my personal devices for taking images of pupils or staff. I note that there is a school mobile phone and iPod available (stored in the school safe) to be used for taking images when on visits outside of school.
12. I will ensure that personal data (including that which is stored in the SIMs database) is kept secure at all times and is used appropriately in accordance with General Data Protection Regulation (GDPR 2018)
13. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
14. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
15. I will report any known misuses of technology, including the unacceptable behaviours of others.
16. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

17. I have a responsibility to limit access to the staff network to staff only. Pupils must never use my network login while accessing any devices.
18. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
19. I have a duty to protect passwords and personal network logins and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
20. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
21. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
22. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety Policy and help children to be safe and responsible in their use of ICT and related technologies.
23. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied, and disciplinary action taken.
24. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead (DSL), the Computing Subject Leader (CSL), or the Headteacher.
25. I will report concerns about the welfare, safety or behaviour of pupils and/ or staff in line with the safeguarding policy and behaviour policy of Ryelands School in line with the 'Responding to an Online Safety Concern Flowchart' (see Online Safety Policy).

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name ……… (PRINT)

Position/Role ………

APPENDIX 8

ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

Ryelands Primary and Nursery School

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

3. I will not use any external device to transfer any data from the school's network.

4. I will respect copyright and intellectual property rights.

5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

8. I will not install any hardware or software onto any school system.

9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied, and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date …….

Full Name ……(PRINT)

Position/Role ………

APPENDIX 9

Ryelands Primary and Nursery School

Ryelands Primary and Nursery School
Torrisholme Road
Lancaster
LA1 2RJ

Telephone: 01524 64626
E-mail: admin@ryelands.lancs.sch.uk
Website: www.ryelands.lancs.sch.uk

Headteacher: Mrs Linda Pye

Online Safety Awareness Session

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Child Online Safety organisations increasingly view Parental Online Safety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event. We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance:

Date:…………………………………………………..Time:……………………………………………………………….

The session will include reference to the following areas with time for you to ask questions:

What are our children doing online and are they safe?

Do they know what to do if they come across something suspicious?

Are they accessing age-appropriate content?

How can I help my child stay safe online?

The session will last for approximately 1¼ hrs where a member of the Local Authority Schools' ICT team will address the issues mentioned above.

Yours sincerely,

<The Headteacher>

I / we will be attending the above Parental Online Safety Awareness Session

Name(s):…….

Parent / Carer of:………………………………………………………………….Year Group…………………………….

APPENDIX 10

Wi-Fi Acceptable Use Policy (AUP)- Parent/ Community Wi-Fi

Ryelands Primary and Nursery School

This is not an exhaustive list and all members of the Ryelands School community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The school provides Wi-Fi for the Ryelands School community.
2. I am aware that Ryelands School will not be liable for any damages or claims of any kind arising from the use of the wireless service. Ryelands School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of Ryelands School.
3. The use of technology falls under the Ryelands School Acceptable Use of Technology Policy (AUP), online safety policy, safeguarding policy and behaviour policy, which all pupils/staff/visitors and volunteers must agree to and comply with.
4. I will take all practical steps necessary to make sure that any equipment connected to the Ryelands School service is adequately secure, such as up-to-date anti-virus software, systems updates.
5. Ryelands School accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the Ryelands School wireless service.
6. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
7. I will not attempt to bypass any of the Ryelands School security and filtering systems or download any unauthorised software or applications.
8. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring Ryelands School into disrepute.
9. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Ms. Kelly Barrett) or the Headteacher (Mrs. Linda Pye).
10. I understand that my use of the Ryelands School Wi-Fi may be monitored and recorded to ensure safe use. If the school suspects that unauthorised or inappropriate use may be taking place, then the school may terminate usage at their discretion. If Ryelands School suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with the Ryelands School Wi-Fi acceptable Use Policy.

Name …………………………………………………………………………………..

Signed: ……………………………………………………………………….Date (DDMMYY)………………