Rudston Primary School and Bright Stars Nursery

Online Safety and Acceptable Use

Including Remote Learning Appendix

Policy Date: September 2020

Staff Lead: Mr J. Griffiths

This policy and all school policies are produced in accordance to guidance set out in our school legislation and guidance policy.

Approved by Governors: September 2020

Reviewed: February 2021

Review: September 2021

Our Mission Statement:

To develop a love of learning, enabling all children

to reach their full potential.

* Respect * Resilience
* Responsibility
* Enjoyment * Challenge *

Safeguarding Statement:

"Rudston Primary school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

1. Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- School Online Safety Coordinator / Officer
- Headteacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors

Consultation with the whole school community has taken place through the following

- Staff meetings
- School Council
- Governors meeting

This Online Safety policy was approved by the Governing Body/Governors Sub Committee :	September 2020
The implementation of this Online Safety policy will be monitored by :	J. Griffiths
Monitoring will take place at regular intervals:	Annually
The Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety policy generated by the monitoring group(which will include anonymous details of e-safety incidents) at regular intervals:	Annually
This policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2021 Reviewed and updated to include Remote Learning AUP Feb 2021
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Headteacher LADO and/or police

2. Scope of the Policy

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place inside and outside of school.

3. Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use

technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

1) Policies and practices

The Online Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the school's approach to Online Safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to Online Safety. The code of conduct forms the basis of the schools expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

2) Education and training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an Online Safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current.

3) Standards and inspection

The school reviews its approach to Online Safety on a regular basis to evaluate and improve its provision.

4. Policy Statements

The school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

As part of the Online Safety policy the school will also manage:

- The use of digital images and video
- Data protection
- Digital communications
- Incidents of misuse

The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care will be taken when capturing digital images and video that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images and videos published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Security and Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act
1998 which states that personal data must be:

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

All school staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly “logged-off” at the end of any session in which they are using personal data.

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies, the school ensures the following good practice:

- The official school email service is regarded as safe and secure. Staff should therefore use only the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat etc) must be professional in tone and content. These communications may only take place on official school systems. **Personal** email addresses, text messaging or public chat/social networking programmes should not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work-related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy

could take place accidentally, through careless or irresponsible or, very rarely, through deliberate misuse.

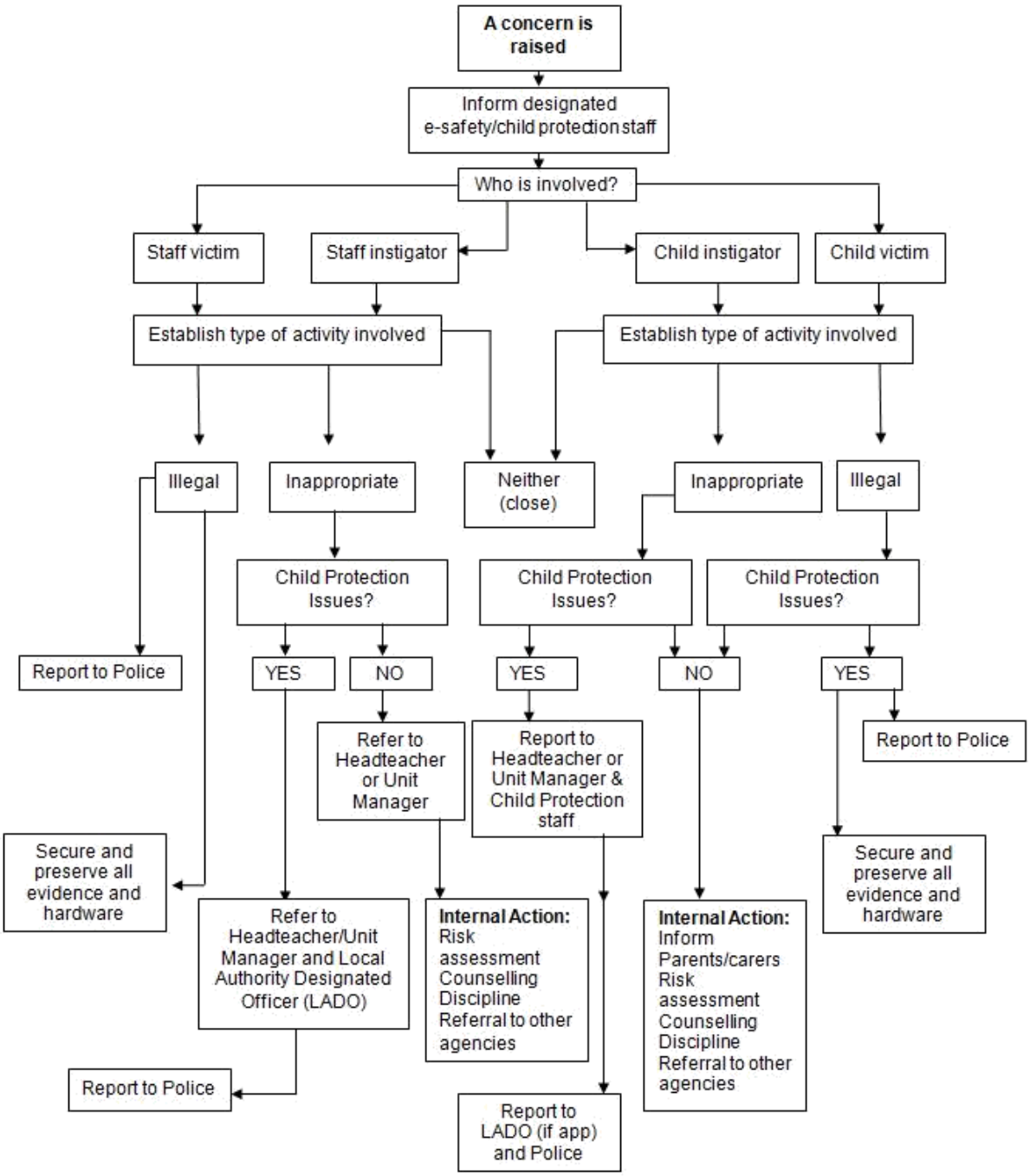
In the event of an online safety incident it is important that there is a considered, coordinated and consistent approach.

Incidents will be managed using the incident flowchart below.

Breaches of this policy and of school AUPs (Acceptable Use Policies) will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Rudston Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform where it is hosted, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The police or other authorities may be involved where a post is potentially illegal or dangerous.



All incidents will be recorded and reported to the relevant parties and organisations.

Pupils Acceptable Use Policy

Keeping safe: Stop, Think, Before you Click!

Rules for Responsible ICT use for KS2

These rules will keep everyone safe and help us to be fair to others.

- I will ask permission from a member of staff before using the internet.
- I will only use websites that a member of staff has chosen.
- I will alert an adult immediately if I find a webpage that is worrying.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will not bring files into school without permission.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will never give out personal information or passwords unless I have been given permission to do so.
- I will never arrange to meet anyone I don't know unless my parent, or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Keeping safe: Stop, Think, Before you Click!

Rules for Responsible ICT use for KS1

These rules will keep everyone safe and help us to be fair to others.

- I will only use the internet and email with an adult.
- I will only click on icons and links when I know they are safe.
- I will only send friendly and polite messages.
- If I see something I don't like on a screen, I will always tell an adult.

Staff/Volunteer Acceptable Use Policy Agreement

To ensure that members of staff/volunteers are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to agree to this code of conduct. Members of staff/volunteers should consult the school's Online Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner, including the installation any software or hardware without permission.

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I will never give out personal details such as home or mobile phone numbers or private email addresses via social networking sites or similar internet sites.

- I will specifically never allow students to access my personal information on social networking or similar sites.

- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.

- I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely – see GDPR policy.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the Online Safety Coordinator (J. Griffiths) or the Designated Safeguarding Lead (A. Mulvaney).

- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

- I understand the importance of upholding my online reputation, that of the school and of the teaching profession), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools.

- I understand that breach of this AUP and/or of the school's full Online Safety Policy and may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff/Volunteer Code of Conduct for ICT.

Signed: …… Print: …… Date: ……

Rudston Primary School - 2020-2021
AUP agreed through Inventry signing in solution

Appendix 1

Remote Learning Acceptable Use Policy

This Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of Rudston Primary School's community when taking part in remote learning following any year group/whole school closures due to Covid-19 and also if any children are self-isolating without Covid-19 symptoms.

Aims

This remote learning policy aims to:

- Ensure consistency in the approach to remote learning for pupils who aren't in school
- Set out expectations for all members of the school community with regards to remote learning
- Provide appropriate guidelines for data protection

Leadership oversight and approval

Remote online learning will only take place using Google Classroom which has been assessed and approved by the Headteacher and Governors.

Contact between the school and parents/carers

Contact with the parents/carers of any child not in school will be through:

- the parent/carer's email address and year group email addresses
- phone calls using the school provided mobile phone or the school landline

Contact with the children not in school will be through:

- Google Classroom using comments, Loom or Mote to give feedback on the children's work.
- Pre-arranged Google Meet sessions for groups of children not in school
- Some phone calls, using the parent/carer's phone numbers, with the parent in attendance and their phone on speaker will be made to support engagement and wellbeing.

Staff will only use Rudston Primary School managed accounts with learners.

- Use of any personal accounts/emails/personal mobile phones to communicate with children and/or parents/carers is not permitted.
- Staff can use work provided equipment e.g. a school/setting laptop, tablet, or other mobile device following the same security arrangements as in the Staff AUP

Roles and responsibilities

Teachers

When providing remote learning, teachers will be at school and will be working their directed hours -Monday to Friday during term-time only. Please note that during partial closure teachers may be teaching in school during these working hours and will not be available at all times during the working day to response to e mails and comments.
If a teacher is unwell and not at school, then other adults will cover the planning and feedback for that class.

All remote lessons will be planned to replicate the normal school timetable for that year group.
Live streamed remote learning sessions will not be held.
When providing remote learning, teachers are responsible for:

- Responding to year group emails from parents/carers
- Providing the learning via Google Classroom
- Checking the uploading has been successful
- Feeding back to children following the agreed policy
- Make referrals to Mrs Mulvaney if work has not been completed
- Reporting any safeguarding concerns to the DSL just as if the learning was taking place in school

Senior Leaders

Alongside any teaching responsibilities, Senior Leaders are responsible for:

- Co-ordinating the remote learning approach across the school
- Monitoring the effectiveness of remote learning – through regular meetings with teachers and receiving feedback from children and parents/carers
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations

SENDCo

Alongside any teaching responsibilities, the SENDCo is responsible for contacting parents/carers of SEND and vulnerable children

Phase Leaders

Alongside any teaching responsibilities, phase leaders are responsible for:

- Monitoring the quality of remote learning – reviewing the quality of the work set in their phases
- Liaising with Subject Leaders and class teachers regarding the quality of work in the specific subjects

Remote learning lead

Alongside the IT Network Manager the remote learning lead is responsible for:

- Fixing issues with systems used to set and collect work
- Supporting staff and parents with any technical issues they're experiencing
- Reviewing the security of remote learning systems and flagging any data protection breaches to the data protection lead
- Supporting parents with access to technology

Office Staff

Office staff are responsible for:
Informing the Class Teacher and remote learning lead (day 1 of absence) by phone of the need for Google Classroom learning if individual children are self-isolating with no symptoms.

Designated Safeguarding Lead

The DSL is responsible for:
Monitoring the safeguarding considerations of remote learning systems and contact between school and home
Mrs Mulvaney is the Designated Safeguarding Lead (DSL).

Additionally, the school have appointed Deputy DSLs who will have delegated responsibilities and act in the DSLs absence:
Miss Walters (HT)
Mrs Cavanagh (AHT)
Mr Robinson (AHT)

Data Protection Officer

The DPL is responsible for:

- Ensuring Google Classroom is recorded in GDPRiS
- Reporting and recording any breaches of data

Mrs McLinden is the Data Protection Lead.

Pupils and parents/carers

Staff can expect pupils learning remotely to:

- Complete the work set by teachers
- Seek help, if they need it, from teachers – either by informing the teacher by private comment on their work on their work or asking their parent/carer to contact their teacher via year group email addresses

Staff can expect parents/carers with children learning remotely to:

- Ensure their child completes the work set to the best of their abilities

- Seek help from the school if they need it
- Make the school aware if their child is sick or otherwise can't complete work

Governing Body

The governing board is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

Data Protection and Security

Any personal data used by staff and captured by Google Classroom when delivering remote learning will be processed and stored with appropriate consent and in accordance with our GDPR and Data Protection Policy.
Emails sent to multiple parents/carers emails are done so using Parent App so they are not aware of the email addresses of others
Not sharing any Google Classroom account details except with the parent/carer of that child.
Ensuring teachers use 141 in front of any telephone numbers when ringing on their work provided mobile
Only members of Rudston Primary School's community will be given access to our Google Classroom Platform.
Children can only access their own class Google Classroom.
Access to Google Classroom will be managed in line with current IT security expectations as outlined in Rudston Primary School's AUPs, and IT Policy and this appendix.

Behaviour Expectations

- Staff will model safe practice and moderate behaviour online during remote learning as they would in the classroom.
- All participants are expected to behave in line with existing Rudston Primary School's policies and expectations.
- Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

Participants are encouraged to report concerns during remote learning:

- For children, reporting concerns first to their class teacher, then Phase Leader, Deputy Head teacher, Head teacher and also telling their parent/carer
- For teachers, to the Phase Leader or Deputy Head teacher, Head Teacher

Inappropriate online behaviour will be responded to in line with existing policies such as Acceptable Use of Technology, Allegations against Staff, Anti-Bullying and Behaviour.
Sanctions for deliberate misuse may include: restricting/removing use, contacting police if a criminal offence has been committed.

Links with other policies

This AUP is linked to our:
Behaviour policy
Child Protection and Safeguarding policy
GDPR and Data protection policy
Privacy notices
Home-school agreement
Online Safety and Acceptable Use of Technology Policy

Policy approved by Governors: September 2020
Reviewed and updated: February 2021
Policy to be reviewed: September 2021