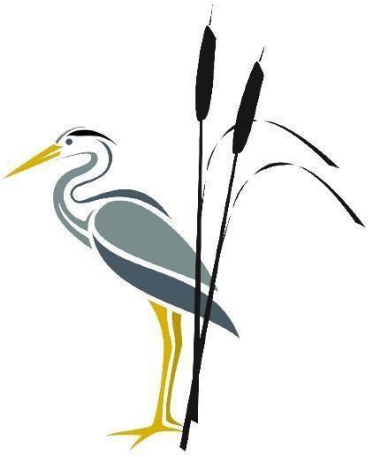
Date: 9/24
Review: 9/26

Rush Green Primary School



Computing policy

safety must follow the school's safeguarding and child protection processes.

Additions made since this document was first produced, are highlighted in yellow.

1. INTRODUCTION AND OVERVIEW

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Rush Green Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken. Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)

Role	Key Responsibilities
Headteacher	• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager
	• To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety To ensure school website includes relevant information. •

Aggressive behaviours (bullying)
Privacy issues, including disclosure of personal information

Digital footprint and online reputation

Health and well-being (amount of time spent online, gambling, body image)

Sexting

Copyright (little care or consideration for intellectual property and ownership)

This policy applies to all members of Rush Green Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Rush Green Primary School

Online Safety Co-Ordinator (Mr Michael)	Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents

	Promote an awareness and commitment to online safety throughout the school Community Ensure that online safety education is embedded within the curriculum Liaise with school technical staff where appropriate To Communicate regularly with SLT and the designated online safety Governor/Committee To discuss current issues, review incident logs and filtering/change control logs

Governors/Safe guarding governor **(Including online safety)**	To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident To ensure that online safety incidents are logged as a safeguarding incident Facilitate training and advice for all staff Oversee any pupil surveys / pupil feedback on online safety issues Liaise with the Local Authority and relevant agencies Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.

Computing Curriculum Leader	To oversee the delivery of the online safety element of the Computing Curriculum To report online safety related issues that come to their attention, to the Online Safety Coordinator. To manage the school's computer systems, ensuring: - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) – access controls/encryption exist to protect personal and sensitive information held on school owned devices - the school's policy on web filtering is applied and updated on a regular basis. That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher.

	• To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	To ensure that the data they manage is accurate and up-to- date Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. The school must be registered with Information Commissioner
Teachers	To embed online safety in the curriculum To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extracurricular and extended school activities if relevant) To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and review annually. The AUP is signed by new staff on induction and all staff when any change is made To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology

	Exit strategy At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually To understand the importance of reporting abuse, misuse or access to inappropriate materials To know what action to take if they or someone they know feels worried or vulnerable when using online technology To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/Carers	To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren to consult with the school if they have any concerns about their children's use of technology to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, on entry to the school.

Regular updates and training on online safety for all staff.

Acceptable use agreements discussed with staff and pupils at the start of each year.

Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents: The school will take all reasonable precautions to ensure online safety.

- Staff and pupils are given information about infringements in use and possible sanctions.
- Headteacher will act as first point of contact for any incident. In his absence refer to Online Safety Coordinator (Mr Michael)
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the

Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

Whether there is an immediate risk to a young person or young people *When assessing the risks the following should be considered:*

Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?

Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?

Are there any adults involved in the sharing of imagery?

What is the impact on the pupils involved?

Do the pupils involved have additional vulnerabilities?

Does the young person understand consent?

Has the young person taken part in this kind of activity before?

If a referral should be made to the police and/or children's social care

If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed

•Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.

•Whether immediate action should be taken to delete or remove images from devices or online services

•Any relevant facts about the young people involved which would influence risk assessment

•If there is a need to contact another school, college, setting or individual

•Whether to contact parents or carers of the pupils involved - in most cases parents should be involved. An immediate referral to police and/or children's social care should be made if at this initial stage:

1.The incident involves an adult

2.There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)

3.What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

4.The imagery involves sexual acts and any pupil in the imagery is under 13

5.You have reason to believe a pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the Headteacher/Named Child Protection Officer is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Our curriculum incorporates aspects of online-safety which provides pupils with the knowledge and skills to navigate the online world as safely as possible for their age group.

The online safety policy is referenced within other school policies (e.g Safeguarding and Child Protection policy, Anti Bullying policy, PSHE, Computing policy).

The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Harmful Online Challenges and Hoaxes

The DFE has released the document entitled 'Harmful Online Challenges and Online Hoaxes (February 2021)

Keeping children safe in Education sets out that an effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establish mechanisms to identify, intervene in and escalate incidents where appropriate.

. EDUCATION AND CURRICULUM

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing and PSHE curriculum areas. This covers a range of skills and behaviours appropriate to their age and experience.
- plans online use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

will remind students about their responsibilities through the pupil Acceptable Use Agreement(s); ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging, use of content, research skills, copyright ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- literature and sessions which contain online safety advice, guidance and training for parents.

3.conduct and incident management expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils; Parents/Carers
- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet

  Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law; • we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Managing IT and communication system

Internet access, security (virus protection) and filtering This school:

- informs all users that Internet/email use is monitored;
- has educational, filtered, secure broadband connectivity;
- uses a filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'Protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup) This school

- Uses individual, audited log-ins for all users – Year 2 and above;
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.

All pupils have their own unique username and password which gives them access to the Internet and other services;

- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
  Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;

- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
  Ensures that access to the school's network resources from remote locations by staff is audited And restricted and access is only through school/LA approved systems:
- Does not allow any outside agencies to access our network remotely except where there is a clear
  professional need and then access is audited, restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;

- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.

E-mail

This school

- Provides staff with an email account for their professional use email and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of technologies to help protect users and systems in the school, including desktop antivirus product Sophos, plus direct email filtering for viruses.

Staff:

- Staff can only use the LA email systems on the school system
- Staff will use LA email systems for professional purposes
- Access in school to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications e.g. Edmodo

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher. They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. Pupils:
- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.
-

Data Security management information system access and data transfer

- **Strategic and operational practices**
- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Equipment and digital content Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- All pupil's mobile devices will be handed in at reception or to the class teacher, should they be brought into school.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Storage, Synching and Access

The device is accessed with a school owned account
The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device. o PIN access to the device must always be known by the network manager.

Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
  Digital images and video In this school:
- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually);
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term, high-profile use

The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work; Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.