Squirrel Hayes
First School

Policy Reviewed on	May 2018	Oct 2018	Oct 2019	Nov 2020	Sept 2021	Sept 2022	Sept 2023	Sept 2024	
Policy Owner Signature	Mrs Johnson Allen	Mrs Johnson Allen	Mrs Helen Johnson Allen	Miss Rebecca Mahan	Mrs Rebecca Percival	Mrs Rebecca Percival	Mrs Rebecca Percival	Mrs Rebecca Percival	
Policy adopted by the Governing Body on	May 2018	13.12.2018	Oct 2019	Nov 2020	Sept 2021	Sept 2022	September 2023	September 2024	
Chair of Govs/Committee Signature									
Policy Reviewed Date	May 2019	Oct 2019	Oct 2020	Oct 2021	Sept 2022	Sept 2023	Sept 2024	Sept 2025	

This school is committed to safeguarding and promoting the welfare of children and young people/vulnerable adults and expects all staff and volunteers to share this commitment.

BIDDULPH SCHOOLS
PARTNERSHIP TRUST
(a mutual co-operative membership trust)

The Schools
Co-operative Society

Squirrel Hayes Online Safety Policy

Rationale

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

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

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Squirrel Hayes First School with respect to the use of COMPUTING-based technologies.
- Safeguard and protect the children and staff of Squirrel Hayes First School and comply with GDPR (General Data Protection Regulation).
- Assist school staff working with children to work safely and responsibly with the internet and other 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.
- Have clear structures to deal with online abuse such as cyberbullying which are 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.

Development, Monitoring and Review

The Online Safety 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.

Should **serious online safety incidents** take place, the following external persons / agencies should be informed:

- The LADO Team

- Police, i.e. PCSO

- Other, i.e. Anti-Terrorism, Social Services

The impact of this policy will be monitored using:

- Safeguarding and Child Protection Incident Forms and logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Internal audits
- Online Safety Learning Walks

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

- **regular meetings with the Designated Safeguarding Lead / Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to relevant *governors group/meeting***
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

Headteacher and Senior Leadership Team

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Online Safety Leads

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particuarly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying and use of social media

ICT Support Team

The ICT Support Team is responsible for ensuring:

- To report any e-Safety related issues that arises, to the Computing Co-ordinator.
- That the technical infrastructure is secure and is not open to misuse or malicious attack.
- That the School meets the required online safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, Internet, remote access, email and any other relevant system is regularly monitored in order that any misuse or attempted misuse can be reported to the Head teacher or Safety Leads for further investigation and for action to be taken where appropriate.
- That monitoring software and systems are implemented and updated as agreed in relevant policies.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up-to-date documentation of the school's e-security and technical procedures

Staff

All members of staff are responsible for ensuring that:

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school

Online Safety Policy and practices

- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to *(insert relevant person)* for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Designated Safeguarding Leads

All DSLs should be trained in online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- hold the lead responsibility for online safety, within their safeguarding role.

- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety & Data Protection Team

The Online Safety & Data Protection Team provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the Online Safety policy including the impact of initiatives. Members of the Online Safety & Data Protection Team are responsible for assisting the Online Safety Leads with:

- The production, review and monitoring of the Online Safety policy and associated documents.
- Mapping and reviewing the online safety curriculum provision – ensuring relevance, breadth and progression.
- Monitoring network / Internet / incident logs.
- Consulting stakeholders – including parents / carers and the pupils about the online safety provision.

Pupils

All pupils should:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy

- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- should know what to do if they or someone they know feels vulnerable when using online technology.

- should understand the importance of adopting 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, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet and mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' meetings, newsletters, letters, the school websites and information about both national and local online safety campaigns. Parents and carers will be encouraged to support the schools in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital images and video taken at school events
- access to parents' sections of the school websites and on-line pupil records (where relevant)

Community Users

Community users who access school systems, websites and so on will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

Policy Statements

Education of Pupils

The internet provides children and young people with access to a wide-range of content, some of which is harmful. As the digital world increasingly becomes a greater part of the learning environment instances of internet misuse are ever on the rise. A real risk to children and young people in the UK today is the process of radicalisation and exposure to extremist propaganda. The internet has been identified as one of the key ways that young people are recruited and conditioned to extremist causes. Extremists for example, use social media and online interaction through these services to share their messages. The filtering systems used in our schools help us to block and monitor any access to inappropriate content, including extremist content. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. We must be aware that children and young people have access to unfiltered internet when using mobile phones and other devices to which they have access outside of school, and may therefore be able to access harmful content such as extremist messages, pornography and other illegal content. With regards to radicalisation, the internet enables connections to be formed through formal and informal groups providing a comparatively risk-free way for potential recruits to find like-minded individuals and network amongst them. The process of radicalisation remains rooted in the real world, and often potential recruits will be encouraged to meet in person but the internet provides a powerful communications mechanism where young people can be reached, groomed and influenced. The internet is therefore a key source of information and propaganda for extremist beliefs. This means that young people can gain access to powerful messages, video and imagery that help to support political claims made by extremists. The internet acts as an 'echo chamber' providing an environment where otherwise unacceptable views and behaviour become normalised through on-going support and encouragement. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the schools to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing, RHE and other lessons and will be regularly revisited throughout the computing curriculum and assemblies.
- Each year group will have explicit teaching in online safety during Autumn 1 and this will be revisited regularly throughout the computing curriculum.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities, including several online safety themed days/weeks each academic year.
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and will be guided to validate the accuracy of information. Staff will reduce the appeal of extremist messages by ensuring that pupils are media literate - making sure that they know how to assess whether material found online is from a trusted source.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how

they can influence and participate in decision- making.
  - Pupils will be helped to understand the need for the Pupil Acceptable Use Policy (AUP) and will be encouraged by all staff to adopt safe and responsible use both within and outside of school.
  - Staff will act as good role models in their use of digital technologies including the Internet and mobile devices.
  - In lessons where Internet use is pre-planned, pupils will be guided to sites checked as suitable for their use as a best practice. Staff will follow the procedures which are in place for dealing with any unsuitable material found as a result of any internet searches.
  - Where pupils are allowed to freely search the Internet, staff will be vigilant in monitoring the content of the websites visited.

<u>Education at home/Remote learning:</u>
Where children are being asked to learn online at home, our school will refer to and use the links and resources provided by the DfE; Safeguarding in schools, colleges and other providers and Safeguarding in remote education.

- Squirrel Hayes will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with learners and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and agreed systems e.g Eduspot (Teacher 2 Parent).
- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our school SEMH/behaviour policy and Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP) and all remote learning will be delivered through Google classrooms.
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

Education of Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, newsletters and the school web sites.
- Parents evenings.
- Parents sessions.
- High profile events and campaigns such as Safer Internet Day and themed online safety days/weeks. Campaigns, advice and information shared with parents will reference relevant web sites and publications such as www.swgfl.org.uk, www.saferinternet.org.uk and www.childnet.com/parents-and-carers.

Education of the Wider Community

Squirrel Hayes First School will provide opportunities for local community groups and members of the community to gain from their online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- Providing online safety information for the wider community on the school websites.

Education and Training of Staff and Volunteers

It is essential that all staff receive regular online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of online safety training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Online Safety Policy and Acceptable Use Policy's.
- The Online Safety Leads will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in team meetings, CPD sessions and INSET days.
- The Online Safety Leads will provide advice, guidance and training to individuals as required.

Governors

should take part in online safety training and awareness sessions, with particular importance for those who are members of any sub-committee involved in technology, online safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by relevant organisations.
- Participation in school training and information sessions for staff or parents. This could include attendance at assemblies and lessons.
- Online based learning courses.

Technical Infrastructure, Filtering and Monitoring

The Head teacher will be responsible for ensuring that Squirrel Hayes' school network infrastructures are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Our schools also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Technical systems will be managed in ways that ensure that the schools meet recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to technical systems and devices.

- All users will be provided with a username and secure password by the ICT Support Team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- The “master / administrator” password for schools ICT system as used by the ICT Leader (technical) must also be available to the Headteacher and kept securely in the school safe.

- The ICT Support Team are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy (AUP).

- The active monitoring system employed in school is regularly updated to flag up a range of key words and phrases, for example, it contains a range of radicalisation words and phrases. This enables full visibility of any possible exposure to harmful content and radicalisation happening within the network.

- Due to the dynamic and changing nature of language, our filtering/monitoring solution provider liaises with a range of expert agencies and partners to ensure that our libraries use up-to-the minute words and phrases that reflect contemporary digital activity. Our libraries are therefore reviewed and updated by our provider on an on-going basis. This aids us in ensuring that pupils are protected from terrorist and extremist influences.

- A Safeguarding and Child Protection Incident system is in place for users to report any actual or potential online safety incident. Staff can obtain a Safeguarding and Child Protection Incident Form from , and must complete and submit this form to an Online Safety Lead or DSL for investigation/follow up within ten minutes of an incident.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the schools systems and data. These are tested regularly. Schools infrastructures and individual workstations are protected by up to date anti-virus software.

- Temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems is subject to their agreement to the Staff Acceptable Use Policy (AUP).
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users).
- The Schools Data Protection Policy covers the use of removable media such as memory sticks, CDs and DVDs by users on school devices. The policy stipulates that whilst any USB memory sticks may be used on school systems for the reading of data, data from school systems will only be writeable to school owned and encrypted USB memory sticks. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (see Data Protection Policy for more). For more details, see the Technical Security Policy.

Use of Digital Images and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet, for example on social networking sites.

Written permission from parents or carers will be obtained before photographs of pupils are published on our websites / social media / local press etc.

In accordance with guidance from the Information Commissioner’s Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the video/images.

Staff are allowed 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 must not be used for such purposes.

Misappropriate use of digital images (such as unauthorised uploading/publishing, i.e. on social media) by staff will be investigated and may result in disciplinary action being taken. Where misuse relates to images of pupils, staff members will be asked to remove them immediately and parents will be informed as soon as is practicable. For more details see 'Responding to incidents of misuse'.

Care should be taken when taking 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.

Photographs published on the 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.

Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. Schools should ensure that they take account of policies and guidance provided by local authorities / MAT / or other relevant bodies. For schools that wish to carry out a more detailed review of their Data Protection policies and procedures SWGfL provides a self-review tool – 360data.org.uk

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The school / academy may also wish to appoint a Data Manager and systems controllers to support the DPO.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities

Staff must ensure that they:

Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, memory stick or any other removable media:

The data must be encrypted and password protected.

The device must be password protected.

The device must offer approved virus and malware checking software.

The data must be securely deleted from the device once it has been transferred or its use is complete.

Communications

Wide ranges of rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff and other adults			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	🟩			
Use of mobile phones in lessons				🟩
Use of mobile phones in social time	Certain locations away from learners- Staff room			
Taking photos on mobile phones / cameras				🟩
Use of other mobile devices, e.g. tablets, games consoles	The use of the school tablets used in class			
Use of personal email addresses in school or on the school network				🟩
Use of school email for personal emails				🟩
Use of messaging apps, i.e. Skype, Facetime				🟩
Use of social media	Use of the school twitter account to be used in class to post what the children have been up to. Google classrooms to update learners on home learning, reading diaries and spellings.			
Use of blogs	Use of blog to enhance the school's profile.			

1 – School owned mobile phones issued to key staff only. An example of use may be during an emergency.

2 – Personal mobile phones must only be used by staff outside of teaching times, and in private spaces only such as the staff room, and not in the presence of any pupils, parents or carers.

3 – School owned mobile phones issued to key staff only.

When using communication technologies, the school consider the following as good practice:

The official school email services may be regarded as safe and secure and are monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.

Users must immediately report to their teacher or a member of staff, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

Pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Personal information should not be posted on the school websites and only official email addresses should be used to identify members of staff.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and

online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. (Schools may wish to consider the use of online/anonymous reporting systems, which can be used by all members of the school community e.g. SWGfL Whisper)
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include

- Non-consensual images
- Self-generated images
- Terrorism/extremism
- Hate crime/ Abuse
- Fraud and extortion
- Harassment/stalking

  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
  - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures

    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged (insert details here). (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
- *governors, through regular safeguarding updates*
- *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"*

Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside of school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

Users shall not visit Internet sites, make, post, child sexual abuse images –The making, production or distribution of indecent images of children - contrary to The Protection of Children Act 1978. grooming, incitement, arrangement or facilitation of sexual acts against children - contrary to the Sexual Offences Act 2003.

Acceptable

Acceptable at certain times

Acceptable for certain users

Unacceptable

Unacceptable and illegal

1 – Online shopping is acceptable in some circumstances, for example, a member of staff making an online purchase on-behalf of school using a school charge card as the payment method would be acceptable

2 – Use of social media for professional purposes only, for example, by staff who manage the school / governor social media accounts.

3 – Staff may use messaging apps only when appropriate to do so. For example, staff may use Skype to deliver training, or to participate in a meeting from one school site with another. Staff with school owned mobile phones may use text messages and video calling to communicate with other colleagues who also have a school owned mobile phone. Staff must never use messaging apps to communicate with pupils or parents. Pupils may use apps such as Skype for video conferencing to communicate with other pupils, or pupils at another school, or in a different country as part of their learning. Use such as this must always be supervised by a member of staff and where necessary, consent obtained from parents.

4 – Use of video broadcasting services for educational purposes only. In the event of publishing any video's online, the School's policy on the use of digital images and videos must be adhered to, and

relevant consent obtained from parents.

Responding to incidents of misuse

All staff are responsible for reporting any suspected misuse or concern to an Online Safety Lead for investigation. This must be done by completing a Safeguarding and Child Protection Incident Form which must be handed in to an Online Safety Lead or DSL within ten minutes of a concern being raised. (For an example form see appendix).

The following guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents (see Responding to Incidents of Misuse in the appendix) and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the Safeguarding and Child Protection Incident Form (except in the case of images of child sexual abuse – see below). once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- Internal response or disciplinary procedures or involvement by Local Authority or national/local organisation (as relevant) or Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour or the sending of obscene materials to a child. o adult material which potentially breaches the Obscene Publications Act. o criminally racist material or promotion of terrorism or extremism or other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

ICT Acceptable Use and Loan Agreement

ICT equipment at home supplied by Squirrel Hayes First School. Use of ICT forms part of the school's approach to Remote/Blended Learning in supporting pupils to continue with their learning if they are physically unable to attend school due to COVID-19 guidelines or other medical reasons.

All organisations (including schools) where computers are in use are required to have a code of practice such as this. It is necessary to outline the principles underpinning appropriate computer use, make expectations clear and ensure all users are fully aware of the consequences of not following the code of practice and indulging in computer misuse.

This acceptable usage policy provides guidance to pupils and their Parents/Carers on what is appropriate use when ICT devices are out on loan. It supplements any legislation around ICT use such as

- Data Protection Act (1998)

- Computer Misuse Act (1990)
- Copyright, Designs and Patent Act (1998)
- Health and Safety (Display Screen Equipment) Regulations 1992 (amended 2002)
- Government guidelines and initiatives such as the Child Exploitation and Online Protection Body (CEOP).

GENERAL COMPUTER USE WHEN ON LOAN:

- School-owned ICT equipment on loan should only be used to access Remote/Blended Learning activities whilst a pupil is unable to physically attend school due to COVID-19 reasons or other medical reasons.
- The equipment will remain the property of Squirrel Hayes First School indefinitely.
- If the parent applies for a place at a different school, at the point of application, the equipment must be returned to Squirrel Hayes First School.
- It is a parent/Carers' responsibility to ensure that there is adequate insurance in place to replace the equipment if damaged or lost whilst in the pupil's possession.

Pupil Accounts:

Parent/Carers are expected to support their child in ensuring that the following is adhered to:

- Pupil accounts are the responsibility of the pupil under the supervision of their Parent/Carer.
- Passwords must be kept secure.
- Pupils must not write their password down or disclose it to anyone.
- Pupils must not allow anyone else to use their account and should not use anyone else's account.
- Pupils must log off or lock their account when away from a machine and must never leave their account logged in and unattended.

Internet Usage:

- Any illegal activity tracked on the laptop/device; including accessing sites meant for adults or gambling sites, will result in the laptop/device being taken away.

- You will not be able to download any material to the school owned property.
- Once pupils return to school full time (following COVID-19) the Pupil/Parents/Carers will return the laptop to school to be reset to its factory settings.
- Monitoring of internet use will take place each week when the laptop is brought into school to be updated.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:
"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…
The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours
Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility
the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- **checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when** a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced **e.g. using SWGfL Test Filtering**

Filtering

- **the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.**
- **illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated**
- **there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective**
- **there is a clear process in place to deal with, and log, requests/approvals for filtering changes** (see Appendix for more details).
- **filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon**.
- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle*
- *the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- **The school monitors all network use across all its devices and services.**

- **monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.**
- **There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.**
- **Management of serious safeguarding alerts is consistent with safeguarding policy and practice.**

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

DOCUMENT CHANGE LOG

Version No.	Date of review	Reviewer	Changes Made
01	Nov 2020	Rebecca Mahan	The use of tablets, social media (twitter) and blogs in school changed. Acceptable use loan agreement added.
02	Sept 2021	Rebecca Percival	Purpose of the policy updated. Updated Governors responsibilities. Updated online safety lead responsibilities. Updated Computer technicians' responsibilities. Updated pupils' responsibilities. The use of Google classrooms added. Education at home/remote learning
02	Sept 2022	Rebecca Percival	Reviewed, no changes made

Version No.	Date of review	Reviewer	Changes Made
03	Sept 2023	Rebecca Percival	Reviewed- Added in DFE guidance for Gov role and responsibilities. Updated the list of Gov role and responsibilities with hyperlinks to documents. Updated online safety lead roles and responsibilities Updated staffs roles and responsibilities Updated DSL's lead roles and responsibilities Updated learners lead roles and responsibilities Addition of filtering and monitoring. Addition of reporting and responding
04	Sept 2024	Rebecca Percival	Reviewed- no changes made