Acceptable use of ICT

&

E-Safeguarding Policy

March 2025

Contents

Acceptable use of ICT & e-Safeguarding

At **Willingham Primary School and Honeypot Pre-School** we recognise that information and communication technology play an important part in learning. All stakeholders in school must use technology appropriately, safely and legally. We have a major responsibility to teach children the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. This policy has links with and works alongside the school's Computing Curriculum; Safeguarding and Child Protection policy; Self-Regulation and Behaviour Management policy; disciplinary rules and procedures; and the Code of Conduct.

Throughout this policy, where 'staff' are referred to, this relates to any individual who has a @Willingham.cambs.sch.uk email address.

1. Responsibility for e-Safeguarding and Appropriate use of ICT

1.1. The Governing Body

- The school governing body have responsibility for ensuring that the school has an Acceptable use Policy of ICT and e-Safeguarding Policy and this policy is reviewed annually.

1.2. The Head Teacher

- The head teacher is ultimately responsible for e-Safeguarding for all members of the school community, though day to day responsibility for e-Safeguarding may be delegated to the e-Safeguarding coordinator.

- The head teacher must ensure that there is a designated person for coordinating e-Safeguarding and acceptable use of ICT, this should be a member of the management team and preferably also a designated person for child protection.
- The head teacher is responsible for ensuring that the e-Safeguarding coordinator receives suitable training to enable them to carry out their role

1.3. The Online Safety Lead

- To promote awareness and commitment to e-Safeguarding throughout the school
- To be the first point of contact on all e-Safeguarding matters
- To take day to day responsibility for e-Safeguarding within school and have a leading role in establishing and reviewing the school's Acceptable use of ICT and e-Safeguarding Policy and procedures.
- To ensure that all staff are aware of the procedures that need to be followed in event of an e-Safeguarding incident
- The Online Safety Lead and technical staff will ensure that all computers have up to date virus protection, monitoring software and an internet connection which is filtered through the Local Authority approved filtering service (Smoothwall).
- The Online Safety Lead and technical staff will meet on a regular basis to discuss monitoring and follow up any arising issues.

1.4. All staff and Volunteers

- All staff have a responsibility to use ICT appropriately and legally and report any illegal or inappropriate use of ICT to the head teacher or the e-Safeguarding coordinator, as soon as possible.
- Teachers and teaching assistants should address issues of e-Safeguarding when using the internet with children

1.5. Technical staff

- To report any e-Safeguarding related issues that come to your attention to the e-Safeguarding coordinator.
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To monitor IT security within the school network and take necessary action to protect its integrity and availability.

1.6. 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 newsletters, letters, website, national or local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to adhere to the following guidelines on the appropriate use of digital and video images taken at school events:

- The school will display a notice advising visitors and parents/carers that mobile phones are not to be used in the setting. If a visitor or parent/carer is seen using their mobile phone, they will be asked to use it away from the children.
- If parents are identified as using the camera function on their phone (outside of events listed below), they will be asked to stop and delete any photos or videos taken.

Exceptional circumstances

- Events that are deemed to be exceptions to the normal policy, will be identified as such by the school prior to the event beginning. Examples will include, but not be restricted to – plays, sports day and assemblies.
- During such events, parents/carers are asked to ensure that any photos or video footage taken must be for personal use only and must not be uploaded to social media websites.
- Where the school identifies that parents/carers have not followed this advice, the school will speak directly to the individuals involved to try and resolve the issue or pass the information onto relevant authorities.

2. Access to ICT

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. The ICT equipment is stored securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware and will be kept active and up to date.

All staff users will sign The Acceptable Use and e-Safeguarding Policy provided by the school. Users must take responsibility for their use and behaviour while using the school ICT systems and must agree that such activity will be monitored and checked.

At Key Stage 1, pupils will access the internet using a class ID and password, which the class teacher supervises. Pupils have individual user accounts for Purple Mash and Numbots. All internet access will be undertaken with a member of staff within the same room.

At Key Stage 2, pupils will have an individual user account for logging into school computers and for curriculum software (TTRS, Purple Mash etc.), with appropriate passwords that will be kept secure. They will ensure they log out after each session.

Members of staff will access the curriculum network using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils, or other adults, to access the internet through their ID and password. Staff will ensure that they understand and abide by their personal responsibilities in relation to the Data Protection Act and associated UK GDPR legislation around the privacy and disclosure of personal and sensitive confidential information. They will abide by the school's Computer Use Rules for Pupils
(Appendix A) at all times.

When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

3. Use of the Internet

The school encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. Internet usage means any connection to the Internet via Web browsing, use of the learning platform, external email or news groups. The school has an obligation to fulfil its Prevent Duty and to ensure that no extremist or terrorist material can be accessed.

The school expects all users to use the Internet responsibly and strictly according to the following conditions and in accordance with the Code of Conduct:

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting extremism or terrorism
- promoting illegal acts
- Other materials reasonably deemed inappropriate for access through school equipment or on a school site.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK
- extremist or terrorist material

Sites must not be accessed that contain inappropriate material, such as that defined below:

- Personal ads or dating
- Criminal skills or resources
- Internet based peer to peer networks, other than those explicitly sanctioned for remote learning use (MS Teams, Loom, Zoom and YouTube)
- Downloads of ring-tones, screensavers and games
- Downloads of freeware, shareware or evaluation packages (excepting by authorised persons as designated by the school and in compliance with copyright law)
- Illegal drugs
- Hacking, virus writing or password cracking
- Gambling
- Depiction or avocation of violence or the use of weapons
- Breach of copyrights
- Instant messaging or online chat rooms not directly related to education or educational use
- Other materials reasonably deemed inappropriate for access through school equipment or on a school site.

Prohibited material will also include any material which may be construed as offensive on the grounds of gender, race, ethnic origin, disability, sexuality, religion, age, HIV status, size, stature, trade union membership/office or any combination thereof or any group identified under the Equality Act 2012.

If inappropriate material is accessed accidentally, users should immediately report this to the head or designated e-Safeguarding co-ordinator so appropriate action can be taken.

Access to internet web sites that are unrelated to school business should be restricted to out of school hours and designated breaks and should not leave a web history through which children may access inappropriate content. Where staff are unsure on whether given content is appropriate, they should contact the e-Safeguarding Co-ordinator for clarity.

The use of YouTube as a teaching tool is allowed, providing staff have vetted the video prior to the lesson to assess that the content is appropriate. Staff should use the freeze screen function when loading the video in case of any adverts appearing that could contravene this policy.

The e-Safeguarding Co-ordinator will ensure that staff are provided with guidance on how to access appropriate videos and Youtube 'safe mode' is set as the default.

Conducting Financial Activities on the Internet

While this policy does not ban the use of the internet for conducting personal financial transactions, e.g. e-banking, we warn against it on school machines. Residual information from such activities can be left on the computer hard drive and could subsequently be accessed by others. Similarly, personal or financial information may be inadvertently recorded by the school's monitoring software. The school or the local authority do not accept any liability for any resulting loss or damage.

Intellectual Property, Plagiarism and Copy Right

Any information copied or downloaded from the internet and then re-presented in any form should acknowledge the source. Any images used should be copyright free.

Email use

E-mail should never be sent, forwarded or replied to where the content is;

- Abusive
- Bullying
- Defamatory
- Disruptive
- Harmful to the school or Local Authority
- Harassing
- Insulting
- Intolerant
- Obscene
- Offensive
- Politically biased
- Threatening

If any of the above are received, whether as direct contact or having been forwarded, staff must report the information in-line with the Whistle-Blowing Policy.

Staff Email

All email messages should include a standard disclaimer stating that the content of the email are not necessarily the views of school or the Local Authority. Any communication with children via email should be through a school email account (e.g. @willingham.cambs.sch.uk). Do not release, or in any way make available, personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses).

The sending of email that are wholly or substantially unrelated to school business should be restricted to out of hours and designated breaks and not completed using a school email account.

2. Photographing

Collection, storage and sharing of personal data, including photographic images of children and young people, is governed by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. Photographic images of children and young people are not automatically considered to be special category personal data:

'The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.'
Recital 51 of EU GDPR, May 2018

This guidance is designed to offer practical advice to schools in order for them to comply with legislation and safeguard the children in their care, whilst enabling families to experience pleasure and pride at their children's achievements through the use of technology.

This policy outlines the safety guidelines for the use of photography and other images of children and young people.

The use of images can be divided into five categories:

- Images taken by the school which are required for the school to perform its public task;
- Images taken by the school which do not fall under the public task purpose;
- Images taken by parents at school events;
- Images taken by the media;
- Images taken by third parties.

Photographs are used in schools for many different reasons and it is important that the different uses are considered separately as they may have different conditions for processing.

If the images taken are necessary for the school to perform its public duty, consent is unlikely to be required. Examples may include: photographs taken of a child in the Early Years Foundations Stage for inclusion in their learning journal; photographs taken to enable staff to identify children with medical conditions/dietary needs; photographs taken of a learning task for use on a school display board.

However, written permission from parents or carers is obtained annually and on entry to the school. A record of children with/without permission for images is held in the school office for the following locations before photographs of pupils are published:

- On the school website
- In the school prospectus and other printed promotional material, e.g. newspapers
- In display material that may be used around the school
- In display material that may be used off site
- Parents and carers may withdraw permission, in writing, at any time.

Pupils and staff will only use school equipment to create digital images, video and sound involving children. In particular, digital images and video will be of appropriate activities and participants will be in appropriate dress; full

names of participants will not be used either within the resource itself, within the file name or in accompanying text online.

Any images, videos or sound clips of pupils must be stored on the school cloud system and never transferred to personally-owned equipment. When staff are accessing the remote desktop from personally owned machine, they're prohibited from downloading such material to their own device. Images must be maintained securely for authorised school use only and destroyed as appropriate when no longer required.

Parents wishing to take images at school events:

Increasingly technology is making it easier for images to be misused and it is therefore important that schools take practical steps to ensure that images of children taken by parents and carers are done so in a way that is in accordance with the protective ethos of the school.

The Data Protection Act does not prevent parents from taking images at school events, but these must be for their own personal use. Any other use would require the consent of the parents of other children in the image.

Examples:

A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply. However, if the photos were posted to a social media page, they must receive permission from the parents of the other children involved.

Grandparents are invited to the school nativity play and wish to film it. These images are for personal use and the Data Protection Act does not apply. However, if the grandparents published the film on their family website/social media page, they must receive permission from the parents of the other children involved.

The head teacher, in consultation with governors, should agree when parents are to be permitted to take images. This information will be communicated to parents/carers at such events.

Social Networking

Staff and children are not allowed to use their personal account on social networking sites, such as Facebook, Twitter or Instagram in school or on school machines unless they have been given permission by Senior Leaders. If staff have social networking accounts, we recommend that their profiles are set to the most private levels. Staff must not have contact with children from our school through social networking sites, other than through the Learning Platform. Section of 8 of the School's Code of Conduct gives further details pertaining to Social Contact and Social Networking.

Staff should not post or make comments on social networking sites that may be interpreted as negative or harmful to the school, its employees, children or the local authority.

Facebook provides support and advice for 'Educators' using Facebook:
http://www.facebook.com/help/?safety=educators

3. Mobile Phones and other Mobile Devices

While mobile phones and personal communication devices are commonplace in today's society, it is recognised that personal mobile phones have the potential to be used inappropriately.

Effective guidance is in place to avoid the use of mobile phones causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice is promoted to protect against potential misuse.

Most mobile phones now offer Internet and email access, alongside messaging, camera, video and sound recording. Mobile phones alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance; however there are also associated risks. Safeguarding of children within the school is paramount.

School staff:

Staff may wish to have their personal mobile phones at work for use in case of emergencies, however there is a clear expectation that all personal use is limited to areas and times when there are no children present, or likely to be present.

• The school expects staff to lead by example and therefore should not make or receive personal calls, or texts (via mobile phone or smart watch), whilst children are present or during contact time.

• Staff (including volunteers and supply staff) should only use their mobile phones and smart devices for personal contact in designated areas such as a staff room.

- Other than in agreed exceptional circumstances, mobile phones should be switched off or on silent and left in a safe place and smart watches silenced during lesson times.

- Staff should not contact pupils or parents from their personal mobile phone in or out of school time, or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, a school telephone should be used. *This is unless teachers are having to work from home during the coronavirus pandemic and would need to contact parents/children to check on their wellbeing – in this instance, staff would need to precede any phone call with a blocking system so their phone number is not shared with parents/carers.*

- Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate

- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this. Staff should not allow themselves to be photographed by a pupil(s).

- In circumstances such as outings and off-site visits, staff will agree with their Line Manager the appropriate use of personal mobile phones in the event of an emergency.

- This guidance should be seen as a safeguard for members of staff and the school. Any breach of school policy may result in disciplinary action against that member of staff.

- Mobile phones should not be brought to staff PD sessions unless explicitly agreed with SMT in advance.

Pupils:

- Pupils are dissuaded from bringing mobile phones to school. If it is deemed necessary for a pupil to bring a mobile phone to school, (e.g. in the case of older pupils because they travel to and from school independently), then the expectation is that the pupil hands their phone into the school office.

- Pupils may not bring 'smart' watches to school. Some watches have the ability to take photos, make and receive calls and messages and present a potential safeguarding issue.

Parents, visitors and contractors:

Parents, visitors and contractors are respectfully requested not to use their mobile phones at all on the school site/in any area where children/young people are present. Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children to avoid any unnecessary disturbance or disruption to others.

Photos of children must not be taken without prior discussion with a member of the Senior Management Team and in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

Any individual bringing a personal device into the school must ensure that it contains no inappropriate or illegal content.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox, RM Portico etc.)

4. Use of Artificial Intelligence (AI)

Willingham Primary School and Honeypot Pre-School expects everyone who uses AI to comply with all relevant laws, regulations, policies and guidelines covering safeguarding, data protection, copyright and other relevant areas.

In implementing and using generative AI Willingham Primary School and Honeypot Pre-School will follow these key principles:

Ethical Compliance: At Willingham Primary School and Honeypot Pre-School we are aware that AI-generated content may possess biases or inaccuracies. We will always review AI-produced results before considering them in academic work. We are committed to ensuring that whenever Generative AI is used bias of all forms will be addressed.

Transparency: We will ensure that pupils, staff, parents and other stakeholders are aware that Generative AI is used in school. This will be communicated via the school website.

Privacy: We will comply with all current data protection legislation ensuring that parental consent is sought and obtained for the use of AI where necessary. We will safeguard all pupil, staff, and stakeholder data. Our Data Protection Policy can be found on our website.

Accountability: Willingham Primary School and Honeypot Pre-School holds itself accountable for the implementation and development of AI systems. The schools Senior Management Team will lead this work and ensure compliance with the guidance.

Access: We will only allow the use of AI with pupils when it has been demonstrated that its use will enhance the experience of students and could improve their outcomes.

Workload: At Willingham Primary School and Honeypot Pre-School we look for ways to better manage the workload of our staff. We will only implement AI when it has been shown that to do so will reduce the demands on staff. AI should enhance, not replace, human creativity. Examples include but are not limited to lesson planning, quiz creation, and worksheet generation.

Responsible use of AI

- Staff must not share personal data with AI tools without approval.

- Staff can use AI tools to support their work as long as no personal data is shared with the tool. Staff must be open and transparent with their colleagues when they have used generative AI to produce curriculum materials. This will allow colleagues to check the reliability and veracity of the resources produced.

- School has conducted a risk assessment in the form of a GDPR compliant DPIA to assess the threat to personal data with the DPO. Approved AI tools include: ChatGPT.

- Staff are expected to use their professional judgement to check any AI generated content for accuracy, bias and relevance before it can be used in the classroom. Staff must not use AI generated content where they have not carried out necessary and appropriate checks.

- Pupils will be taught about the opportunities and risks arising from the use of Artificial Intelligence in ways appropriate to their age and educational key stage.

- Pupils will be taught the importance of critical thinking, creativity and originality in their work. Pupils who use generative AI to produce work must acknowledge and reference the tools they have used and the work that it has produced.

- Pupils will be taught how to use generative AI ethically and to avoid it being misused.

- Pupils will be taught about the threats posed by AI and will be expected to apply the knowledge they have regarding copyright, intellectual property and plagiarism to ensure that their use of AI is ethical and legal and complies with the existing legal framework.

- Pupils will be taught how to keep themselves and others safe whilst using AI and will be expected not to use AI in an unsafe manner. Whenever a pupil uses AI in an unsafe way that causes harm to themselves or others, they will be dealt with in accordance with the school's behaviour policy.

5. Online Safety Curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

At Willingham Primary Scool and Honeypot Pre-School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the Internet. Our online safety curriculum is based on evidence-backed Purple Mash platform and associated tools and software required to teach the computing schemer of work with national curriculum coverage.

Other uses of internet

Purple Mash, Timestables Rockstars and Numbots use individual log-ons and passwords for all children. All adults have individual logon and passwords to both the school network and the Centrally Hosted system. User names and passwords must be kept secret and not shared with other users. All accounts are filtered through the online filters with inappropriate content being blocked. If a child or adult forgets their username or password, this can only be reset by **Meridian or Jo Aldhouse.**

Filters are set differently for students and teachers to allow appropriate access.

Staff are able to save and share work/resources through the use of Microsoft Teams.

Teachers should follow the national curriculum for Computing and ICT.

There are times in the week when children have 'free' use of the school network, such as during computer clubs, wet playtimes, reward time for good behaviour etc. However, this access is still supervised by an adult. Any games played on the school network must be in line with the school rules and be suitable for primary aged children.

Children should not download music onto the school network. If music is free to download it is usually illegal. Staff may download music, but this must be done legally, in line with copyright laws and for use within school e.g. from the Sing-up website and can only be completed by a 'Power User'.

6. School's online presence

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. The school obtains parental permission before using images of pupils. We ensure the image file is appropriately named – we do not use pupils' names in image file names or ALT tags (Alt tags are the labels that describe the images on a website) if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. We will use group photos rather than photos of individual children, wherever possible.

The school occasionally promotes news and events through Twitter. Staff given access to post by Senior Leaders should adhere to the following points:

- Ensure posts reflect well on the school.
- Never refer to a political preference
- Do not use the names of pupils where their photo is present
- Check posts carefully before submitting, where possible checking the content with a colleague
- Report any unwelcome comments by visitors to the Head teacher or Deputies
- Ensure photos have been checked against the school's permissions list

7. General Data Protection Regulations (GDPR) and the Data Protection Act 2018

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 which state that personal data must be:

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

8. Filtering and Monitoring

The school uses a software package (Net Support) on the curriculum network which monitors the use of ICT and the Local Authority provide filtering through Smoothwall. This software will;

- Log all computer activity to a central database
- Monitor and record an unlimited number of screens in real-time
- View current and previously opened windows, websites, applications, printed documents and deleted files
- Detect written keywords or sentences with screenshot or video evidence
- View evidence of attempts to access banned windows, websites and applications
- Instantly alert you of violations such as attempts to access banned websites
- Perform a number of operations such as logoff or send email upon violation detection

Internet traffic is monitored through Smoothwall. The Designated Safeguarding Lead receives notifications of activities that may represent a safeguarding risk.

9. Breaches of this policy

Breaches of this policy will be dealt with in line with the school's Code of Conduct and Disciplinary Rules/Procedures for staff; and with the Self-Regulation and Behaviour Management Policy for pupils.

10. Remote Education

The school has a Remote Education Policy that covers all aspects of Remote Education provision for pupils. Appendix B holds a risk assessment for online meetings and lessons.

Appendix A Reporting and dealing with incidents

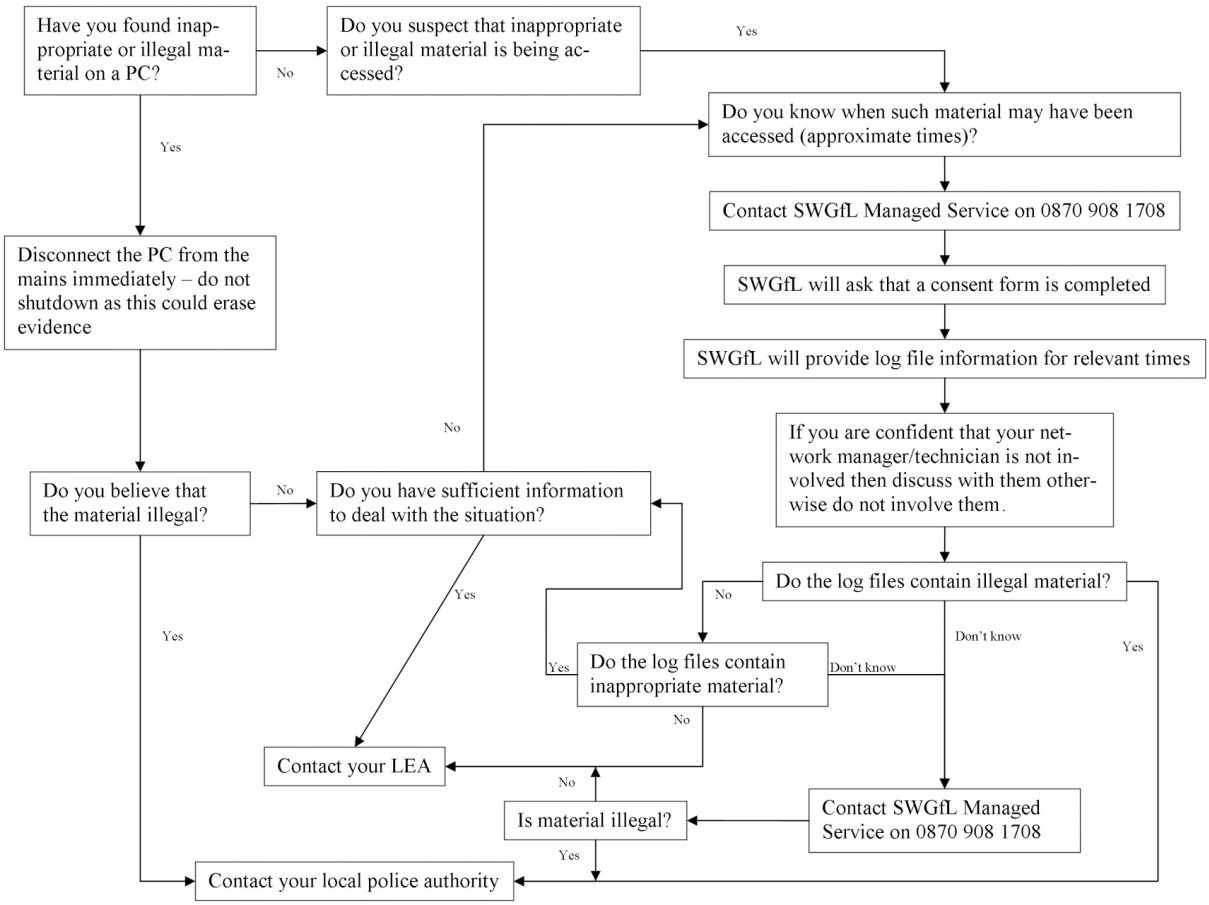
Incidents of concern must be reported to the e-Safeguarding Coordinator or the Headteacher.

Any concern regarding children's safety to the Designated Child Protection Coordinator.

If you find inappropriate or illegal material on a PC or other electronic device in school, do not try to capture or copy evidence, this may leave you in the position of distributing illegal images. Ensure children cannot access the inappropriate or illegal material - turn off the screen, remove the device to a secure place or switch off power at the wall. You then MUST report this to the e-Safeguarding coordinator.

This flow chart is produced by South West Grid for Learning. It will be used as a guide for senior managers on how to deal with any incident.

Please note: our contact is **the headteacher,** not SWGfL as on the flowchart.



Appendix B Risk Benefit assessment of remote learning and working

Risk Benefit Assessment online video meetings and lessons

Generic Benefits	Generic Safeguards
• Increased engagement from pupils • Ability to 'teach' new content • Safeguarding – ability to see individual children in their home setting • Support for parents at home	• Staff to follow WPS Safeguarding Policy guidance • Staff to follow Government Online provision guidance • Staff to follow "Guidance for safer working practice for those working with children and young people in education settings Addendum April 2020" • Application for Disadvantaged laptops for eligible families

Specific Activity	Possible Problems/Issues	Probable Benefits	Control measures, reasonable and practical steps to avoid or reduce problems/issues	Decision/Comments/Actions
Weekly Zoom Meetings	• Attendance of non-invited individuals • Pupils making inappropriate comments • Safeguarding of pupils • Safeguarding accusations against staff • Non-access for Disadvantaged pupils • Pupils in school missing out on lessons	• Increased engagement from pupils • Ability to 'teach' new content • Safeguarding – ability to see individual children in their home setting • Support for parents at home	• See Zoom Meeting Protocol for further details • Passwords to be used for all meetings (changed each meeting) • Disable join before host • Participants to be held in a waiting area to be admitted by the staff • Mute pupils on entry and throughout the meeting unless teacher unmutes pupil for a question or response • Disable written chat between participants • Record sessions as default • Follow up phone call to pupils not in attendance or in onsite provision • Teachers and pupils to be in a 'public' location in their house –	Go ahead with activity with the safeguards in place Staff to be trained on scheduling meetings with the appropriate settings Protocol to be written and shared with staff to remind them of how to set meetings up with appropriate safeguards.

			not bedrooms. If staff have to use a bedroom, they should use a 'virtual background' to blank this out • Use of iPads in classrooms for onsite pupils to access the sessions regularly (although not guaranteed weekly) • Letter to parents to re-emphasise the importance of password security and the need to not share links or passwords with others	
Use of Loom to create lessons with new content	• Sharing of WPS content widely on the internet – Teacher wellbeing • Pupils not able to access content • Non-access for Disadvantaged pupils • Accidental sharing of content in the background of video	• Increased engagement from pupils • Ability to 'teach' new content • Safeguarding – ability to see individual children in their home setting • Support for parents at home	• Disable comments on both Loom site and YouTube uploads • Weekly phone calls for pupils not accessing work to 'check-in' and support • Teachers to ensure that all other apps and sites are closed and notifications are turned off before recording • Videos to be reviewed for accidental content by creator before uploading and sharing • Upload to YouTube for greatest accessibility	Go ahead with activity with the safeguards in place Staff to be trained
Uploading of staff videos to YouTube	• Staff not happy about being on YouTube • Footage of staff and their home environment shared on the internet • Inappropriate comments seen by pupils/staff about the videos • Inappropriate adverts seen by pupils	• Increased engagement from pupils • Ability to 'teach' new content • Safeguarding – ability to see individual children in their home setting	• Staff choice of whether to feature in videos • Ability for people to comment on videos to be turned off in publisher's account settings • Videos to be set as 'made for kids' by default to remove advertising • Teachers to consider carefully the filming of their videos to	Continue with activity with the safeguards in place

	• Non-access for Disadvantaged pupils	• Support for parents at home	avoid any personal information being shared	
Live or recorded lessons/assemblies	• Footage of children shared on the internet • Inappropriate comments seen by pupils/staff about the videos • Inappropriate adverts seen by pupils • Poor behaviour seen by parents • Non-access for Disadvantaged pupils	• Increased engagement from pupils • Ability to 'teach' new content • Support for parents at home	• Pre-recorded lesson footage reviewed before uploading – any footage that is deemed to put any pupil or the school 'at risk' not to be used • Use of Teams to share through MS Stream or within Class Teams • Parents able to remove pupil from any video footage recording and request that they do not appear on published videos • 'Live' lessons/assemblies to not include pupils in the room – to use Zoom and follow the 'zoom protocol'	Go ahead with activity with the safeguards in place
Use of MS Teams to share work and content	• Chat between pupils in Teams • Non-access for Disadvantaged pupils	• Increased engagement from pupils • Ability to 'teach' new content • Support for parents at home • Provides pupils with access to MS Office 365 applications • Ability to share content, including videos less publically than YouTube	• Chat/call facility turned off for pupils • Ensure password reset is enabled for pupil • Ensure Outlook is turned off for pupils	
Shared with Governing body on:			Shared with Staff on:	