Online Safety Policy

Policy Review

This policy will be reviewed in full by the Governing Body on an annual basis.

This Policy was last reviewed and agreed by the Governing Body on:

Chair of Governors Signature:

Executive Head teacher Signature:

Date: Jan 2026
Review: Jan 2027 or sooner should any changes occur

This page left intentionally blank

Contents

Introduction 5
Monitoring Software 5
Online Safety in the curriculum 7
Lower Key Stage 2 7
Upper Key Stage 2 7
Remote education 7
Governors 7
Parents and Carers 7
Visitors to school 8
Communication within school 8
Mobile devices 9
Digital images in the school community 9
The Internet 10
Use of digital cameras including CCTV / iPads 10
Media Publications 10
Ownership of Images and Footage 10
Social networking and personal publishing 11
Social Media - Protecting Professional Identity 11
Protecting personal data 12
Authorising Internet access 12
Handling Online safety complaints 12
Staff and the Online Safety Policy 13
Responding to incidents of misuse 13
Other Incidents 15
Appendix 1 – Staff Acceptable Use Policy Agreement 16
Appendix 2 - Pupils Acceptable Use Policy 18
Appendix 3 - Visitors Acceptable Use Agreement 19

This page left intentionally blank

Online Safety Policy

Introduction

The Online Safety Policy relates to other policies including those for Computing, Anti -bullying and for Safeguarding.
Palfrey Junior School's named Online Safety Coordinators are: Emily Kinsey (HOS Online Safety Coordinator DSL), Cheryl Collis (HOS and DSL) and Laura Smith (Computing and Online safety lead)

Our Online Safety Policy has been written by the school, building on advice received and government guidance. It works in conjunction with the school's acceptable use policy. It has been agreed by senior management and approved by governors.

The school will monitor and enforce the policy through:

- Teacher planning
- Smoothwall monitor– monitoring of network activity for laptops and desktops. The use of iPads in class needs to be monitored, pupils to use pre-determined websites and apps and Securus software monitors internet activity.
- Records of any incidents
- Online safety survey for children
- Online safety team at Walsall Education
- Network Manager to ensure all security software, including virus software and settings are kept up to date (LA ICT)

Every member of the school community has a duty of care to online safety as part of safeguarding. This policy deals with incidents associated with the use of technology that affects our school community.

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities.

Online Safety Incidents that occur outside of school are covered by parents' duty of care, including social media such as What's app. Unless it brings the school into disrepute, mentions staff or pupils by name, then school can intervene.

Monitoring Software

Smoothwall Monitor through Walsall Council Online Monitoring service across the desktop, laptop and chromebook network in order to:

- Monitor inappropriate use of language and behaviours.
- Monitor internet usage including words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy
- Monitor device use to ensure all appropriate activity

Securus monitoring is used for iPad internet activity. This Soley monitors the internet activity on the iPads. This means that iPad activity should be physically monitored in classrooms so that we ensure children are not accessing inappropriate content and behaving appropriately.

This is monitored by Walsall Council Online Monitoring service and reviewed by the Local authority Online safety advisor in order to ensure that all staff and pupil conduct is monitored effectively.

Any identified incident is reported to Cheryl Collis and Emily Kinsey as Heads of school, in order for it to be investigated and dealt with. Incidents of every level are also monitored and reported by the Local authority Online Safety advisor and reported via email. Level 5 incidents are followed up with a phone call and the advisor expects a return email to acknowledge receipt of reports.

A weekly report that is a reassurance email that gives an update on the number of users (people who log into devices), the number of devices that are being monitored and number of captures in the week. A monthly report is sent that includes details relating to school captures and incidents. This helps and supports us to identify the risk profile and look at patterns in the captures.
The monitoring software does not negate the need for staff to supervise pupils when using devices and it should be noted that it works on networked devices and chromebooks but not iPads. iPad use should be fully supervised by staff and websites given to pupils in order to reduce the risk of coming across inappropriate content.

Chromebooks and networked devices are filtered through network access via Fortinet. They are monitored using Smoothwall monitor. This works at a user level rather than a device level so will capture when pupils login on google accounts using personal devices, school will be mindful of this and report incidents as appropriate to parents/carers.

Managing filtering

The school will work with LA ICT support to ensure systems to protect pupils and staff are reviewed. The school use Fortinet software as a technical monitoring solution. This allows differentiated internet access for staff, pupils and guests. If staff comes across unsuitable on-line materials, the site must be reported immediately to the online safety Coordinator. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the DSL/Online Safety Coordinator via CPOMS, they need to record the website and what device they were on so that the Heads of school can report this to the technicians. Staff are now able to access sites such as 'You Tube' and others on request by the Heads of School but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. Staff should either download the video before lesson or pause the video after the adverts and before it ends to prevent the adverts and 'up next' video.

Links and content should be checked in school just prior to use in the classroom due to daily rotation of advertising content and ability to access in school. Children should be given websites to look at and not be allowed to freely search the web without teacher supervision, ideally using 'Kiddle' the search engine.

Laura Smith, Online safety lead will ensure that the school's filtering system is working by randomly checking logins and devices, half termly, using 'test filtering' www.testfiltering.com. A screen shot of the checks will be made and saved on the school's network. This is recorded on a spreadsheet and stored on the school network.

Online Safety in the curriculum

A programme of training in Online Safety will be taught to children across the school, every half termly. Online Safety training will be included within the Personal Social and Health Education (PSHE) curriculum and children will be reminded at the beginning of any session using devices about online safety. School have planned a progressive curriculum based on Purple Mash 2 Be safe resources that staff can teach, this has been mapped against the Education for a Connected World objectives to ensure it meets the requirements of the standard set in Keeping Children Safe in Education 2025. Pupils are then required to take a quiz to assess current learning capability. These are the behaviours that children need to learn as part of the statutory curriculum for Online Safety.

Lower Key Stage 2

Children are given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc.). They will be shown how to develop a responsible attitude towards searching the internet and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Upper Key Stage 2

Children are encouraged to become more independent, agreeing to the acceptable use policy first, before searching for information on the internet using a child friendly search engine, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Remote education

Remote education is included in our safeguarding considerations please consult our remote learning policy for more information. This is available on the school website as a statutory requirement of the school.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the Online Safety Policy. In accordance with KCSiE September 2025 Governors should ensure they have had training on an annual basis about online safety.

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. Palfrey Junior School will take every opportunity to help parents understand these issues through parents' evenings, newsletters (including updates from the digital leaders), letters, website and information about national and local online safety campaigns. Palfrey Junior school invite parents to work with their children around online safety in a session led by the Local Authority Online Safety advisor and the Palfrey Protectors/Digital leaders. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- their children's personal devices in the school (where this is allowed, to be agreed by SLT)

Where an incident occurs within school the child's parents will be given appropriate advice for the use of technology at home. If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

Visitors to school

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

This will be displayed and accepted during the sign in process.

Communication within school

Pupils may only use approved electronic communication accounts on the school system. (E.g. google classroom). Pupils will be told they must immediately tell a member of staff if they receive an offensive message.

Staff should use a school agreed communication systems e.g. email for anything work related and no other email address. The forwarding of chain communications is not permitted. Staff should not use social media to discuss work and pupil issues.

Mobile devices

The use of mobile devices by staff including mobile phones should not be in the classrooms especially during the school day (8.30 – 3.15) excluding lunchtimes in the staff room and only used on school trips away from children in an emergency. All Staff devices including smart watches should be silenced, notifications disabled during school hours and children prevented from reading anything on the screen of the device. Staff use of personal devices, including mobile phones, will not be used during lessons or formal school time unless express permission is given by the Heads of School. Personal devices must not be accessed when children are present. The sending of abusive or inappropriate messages or files by Bluetooth or any other means is forbidden. Staff will be issued with a school phone where contact with pupils/parents is required. Staff will not use personal devices to capture images/videos of pupils.

We do not allow children to bring mobile devices into school. This policy applies to the use of mobile phones as cameras in all circumstances.

Digital images in the school community

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's 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 e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of only 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 / made publicly available on social networking sites, nor should parents and carers comment on any activities involving other pupils in the digital and video images. Parents will be reminded of this at the beginning of any events where they are able to take images/videos.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images which prohibits such activity. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed (e.g. school uniform or PE kit) 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. For example, a child must ask another before taking their photo. Free time on

computers and iPads must have guided access and /or only allowed to access certain websites and apps, decided before hand by the teacher.

- 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, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website, class teachers hold a list of these permissions too

The school will observe the way in which video recordings are made and photographs taken, during performances, and will withdraw the right of anyone to bring in a camera of any sort if they are felt to be making inappropriate images. For example, photography is forbidden in changing rooms or backstage during school productions.

The Internet

Only appropriate images will be used on the school internet site, and children will not be identified by their name or address on the school website.

Use of digital cameras including CCTV / iPads

There are many ways in which the use of digital images is valuable for children's learning. For example, they may be used in art work or geography or science fieldwork. Images will be made only as appropriate for school-related activities. Children will be taught how to take pictures, but we will discourage them from taking pictures of each other, and they will be supervised by an adult when they have access to a digital camera.

As soon as images have been used for their intended purpose they will be deleted. The school will not store digital images any longer than for their immediate use.

Media Publications

Sometimes, local or national media visit the school to follow up a news story. This is often to do with a notable achievement by a child or a group of children from the school. For example, sports competition, or the school may have raised money for a charity. In this situation, where children's images might be made public, the school will inform the parents of the event in advance, and allow them to withdraw their child from the event if they so wish. Newspapers normally ask for the names of the children to go alongside the photographs; if parents or carers do not wish this to happen, then the school will not allow the individual to be photographed or filmed by the media concerned.

Ownership of Images and Footage

Any images collected by employed staff during school time and events are 'owned' by the school and it remains the school's responsibility to store or delete the images securely once they have been used and never to pass on images to a third party. No rights to images can be claimed by outside agencies or the representatives of individuals. The school reserves the right not to allow images of the school and its community to be used for any purpose beyond education of the pupils, regardless of parental consent, if there are overriding reasons. External groups must apply in writing to the Governing Body for use of images belonging to the school. Parents/carers may request copies of images stores by the school, provided their own child is in the image.

Social networking and personal publishing

Pupils will be educated in the safe use of social networking sites alongside the use of relevant child friendly websites.

Pupils, staff and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised to use nicknames and avatars when using social networking sites. Staff must not make 'friends' or communicate with current pupils and their parents or pupils that have left on any social network site, i.e. Snapchat or Instagram. Staff should check that their privacy setting is set to Friends only/Private. Staff who choose to use social network sites do so at their own risk and should be aware of the School's Code of Conduct, Acceptable Use Policy and Professional Standards.

Pupils will be taught when 'gaming', they should only communicate with people they know rather than unknown gamers as well as only playing age appropriate games.

If something makes pupils worried, scared or sad they will be reminded to report to trusted adults, Childline or CEOP.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information: Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk School staff should ensure that:
- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

School social media accounts:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:

  -Systems for reporting and dealing with abuse and misuse

  -Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or

impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites on own mobile devices during non-teaching time only.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Refer to the School's data handling policy.

Staff should not walk away from any device without first locking it (Windows key and L)

Memory sticks are discouraged to be used, where they are used they should be encrypted and password protected. All staff laptops are encrypted. Google Drive/Classroom is the preferred method to be used to share files between staff to access at home and to communicate with pupils.

Authorising Internet access

Parents will be asked to sign and return a consent form on entry to the school allowing pupils to use internet for educational purposes.

Handling Online safety complaints

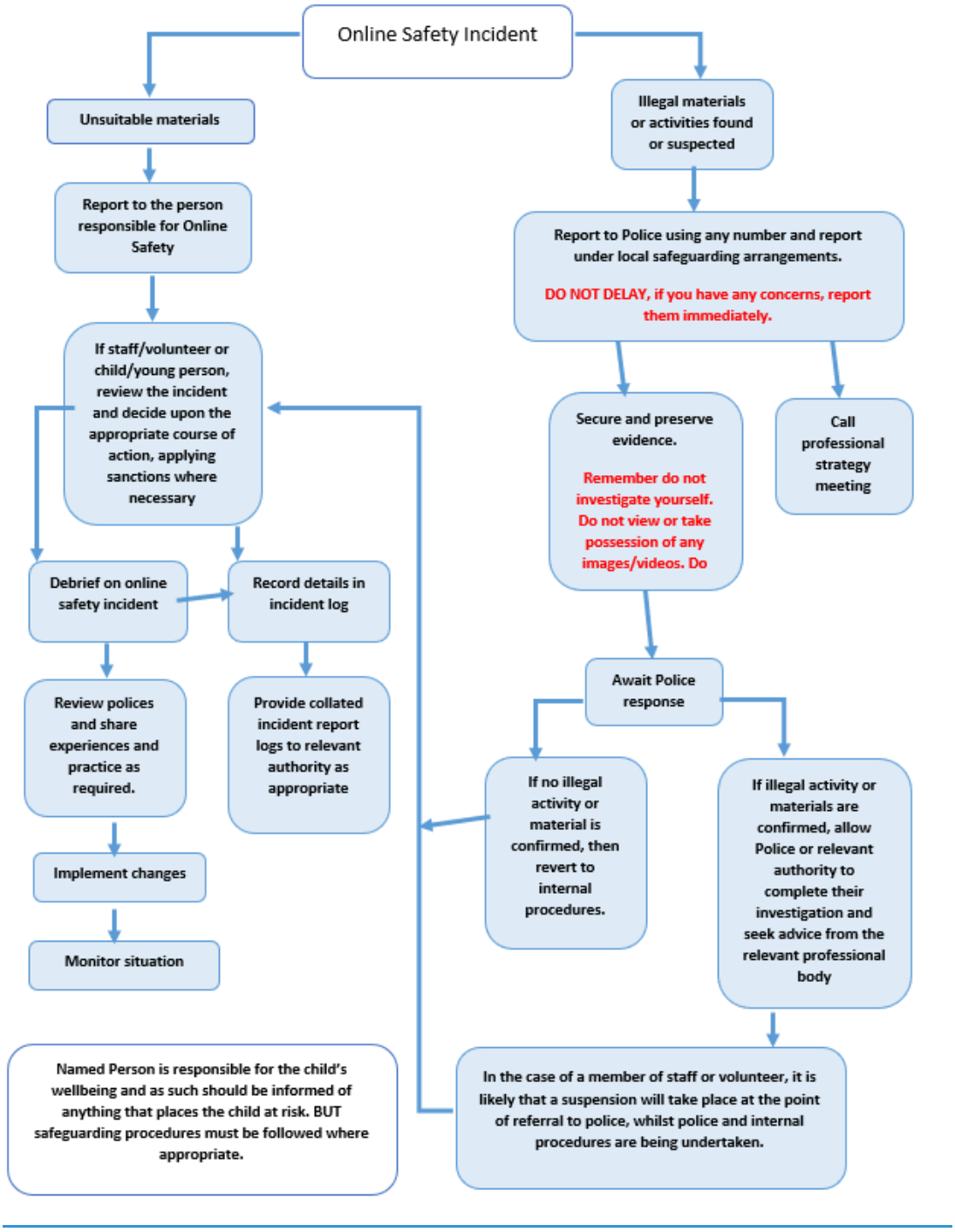
- Complaints of internet misuse will be dealt with by an online safety coordinator or a senior member of staff. Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Any complaint about staff misuse must be referred to the Heads of school or LADO (Belinda Crowshaw)
- Complaints of a safeguarding nature must be dealt with in accordance with school's safeguarding procedures.
- Peer to Peer abuse - the school recognises that safeguarding issues can manifest themselves via peer on peer abuse. Online bullying/incidents will be dealt with in line with the schools Safeguarding and / or Anti Bullying Policies.

Staff and the Online Safety Policy

All staff will receive in house Online Safety update training on an annual basis. Staff are informed that network and internet traffic will be monitored and can be traced to the individual user.

Responding to incidents of misuse

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 (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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 / volunteer 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 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 discipline procedures
  - Involvement by Local Authority or national / local organisation.
  - 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
  - the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
- 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.
- All staff to report any online safety issues using **CPOMS**

Appendix 1 – Staff Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communication systems.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by school.
- I will not disclose my user name or password to anyone else, nor will I try to use any other person's user name and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I should change my password regularly (at least once a year) and they should be secure passwords made up of 3 random words, numbers and symbols.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile devices (laptops / tablets / mobile phones / USB devices, smart watches etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others, I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal information is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted Data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that this Acceptable Use Policy applied not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or The Local Authority and in the event of illegal activities, and the involvement of the police.

Appendix 2 - Pupils Acceptable Use Policy

KS2 Acceptable use Policy

Staying safe whilst using the computer

To help me stay safe on the computer...



I will ask permission before using the Internet and use it for a specific purpose.



I will never share my personal details, such as my full name or address, with people I don't know.



I will never share my password with anyone.



I will never meet up with someone I have met on the Internet.



I will always check my messages are polite before I send them.



I will not reply to a message that isn't kind, but I will save it and show it to an adult.



I will not open or download a file unless I am sure it is safe.



I know I should not believe everything I read on the Internet.



I will always tell an adult if something on the Internet makes me or my friends unhappy.

Appendix 3 - Visitors Acceptable Use Agreement

I understand that I must use the school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring in to the school:

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting, including mobile phones.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others, I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that if I take and / or publish images of others I will do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish, or share any information I have obtained whilst in school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment, or school software, however this may have happened.
- I will ensure that I have the permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices.