Whitstone Community Primary School

Online Safety Policy

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, who have access to and are users of school ICT systems.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

This policy should be read in conjunction with the school's
policies on:
Bullying,
Safeguarding,
Behaviour,
Data Protection and Computing.
Equality & Diversity

Roles and Responsibilities

Governors / Board of Directors:
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

The Online safety governor is **Mr Freeman**

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-Ordinator
- regular monitoring of online safety incident logs
- reporting to Governors,

Designated Person for Safeguarding and Child Protection

The designated person for child protection, Mrs Mould (Head teacher) ia trained in online safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Head teacher and Senior Leaders:

The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online-Safety Co-Ordinator.

- The Headteacher (Mrs Mould) and Online Safety coordinator are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Head teacher will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with school technical staff (NCi);

•receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments;
•meets regularly with the Online Safety Governor and members of the governing body to discuss current issues, review incident logs;
•reports regularly to the Head teacher;
•regularly monitors the school's online profile.

Technical Staff (NCi)

The ICT Technician is responsible for ensuring that:

•the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
•users may only access the school's networks through a properly enforced password protection policy;
•shortcomings in the infrastructure are reported to the Computing coordinator or head teacher so that appropriate action may be taken;
•that the use of the *network / internet / email* is regularly monitored in order that any misuse / attempted misuse can be reported to Mrs Mould (Headteacher) / (Online Safety Coordinator) for investigation / action / sanction.

Teaching and Support Staff:

are responsible for ensuring that:

•they have an up to date awareness of online safety matters and of the current school e-safety policy and practices;
•they have read, understood and signed the Staff Acceptable Use Policy;
•they report any suspected misuse or problem to Mrs Mould (Headteacher. Online Safety Coordinator for investigation. When doing this incidents should be recorded in the Online Safety log (further details can be found at the end of this document);
•all digital communications with students / pupils/ parents / carers should be 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;
•pupils understand and follow the online safety and acceptable use policies;
•pupils have a good understanding of research skills;
•they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;

•in lessons where internet use is pre-planned pupils should be 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. Older children should also be taught how to carryout 'safe' searches.

Pupils:

•Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy;

•have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

•need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

•will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying;

•should understand the importance of adopting good e-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 / Carers

•Should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online-Safety acceptable use agreement form at time of their child's entry to the school;

•Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good e-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).

For further information about e-safety please visit the website below.
http://www.childnet.com/parents
Additional websites and up to date information can also be found on the school website.

Education–pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online

safety is therefore an essential part of the school's / academy's online safety provision. Children and young people need the help and support of the school 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. At Whitstone C.P. School staff Online safety is provided through our Computing and PSHE rolling programme and cross-curricular opportunities are also used. In addition, assemblies and special events are also used.

When delivering sessions on online safety pupils:

- should be taught to acknowledge the sources of information that they use and respect copyright when accessing material online.
- Students / 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.
- revisit topics regularly;
- be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information;.
- should be encouraged to adopt safe and responsible use both within and outside school. Key stage 2 pupils will understand and sign the Acceptable use policy;
- staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- staff should understand that in lessons where internet use is pre-planned, it is best practice that students / pupils should be 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;
- should be shown how to carry out safe searches if they are allowed to freely search the internet; staff should be vigilant in monitoring the content of the websites the young people visit and support them in the use of keywords that will help them access age-appropriate websites.

Education –parents / 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 / regulation of the children's online 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. This may be done through:

- Letters, newsletters, the school website
- Parents / Carers evenings /sessions
- High profile events
- Reference to the relevant web sites / publications eg.
- www.swgfl.org.uk
- www.saferinternet.org.uk/
- http://www.childnet.com/parents

Staff/ governor/ volunteer training

This school:

- Ensures that members of the school community know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection (for further information, see the school's Data Protection Policy);
- Makes regular training available on e-safety issues and the school's e-safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience], governors and volunteers with information and guidance on the Safeguarding policy and the school's Acceptable Use Policies.
- Shares regular updates with staff, through Online Safety's Co-ordinator attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- Ensures that this policy and updates will be presented to and discussed by staff in staff team meetings / INSET days.

Communications

At Whitstone School the internet will be used to communicate with others in a range of different ways, including through: emails, blogs and webcams.

Users must immediately report, to the nominated person (Mrs Mould-headteacher), 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. The school will contact the Police if a member of staff/ pupil or school receives any form of communication that is considered to be particularly disturbing or that breaks the law.

Emails:

Whitstone School uses Outlook 360 to provide children (shared class account) and staff with email accounts. These official school email services may be regarded as safe and secure and are monitored.

Children:

- At Whitstone School children use class accounts, run by Outlook 360.
- In school they will only be able to communicate with individuals who have been approved by members of staff.
- Will be made aware that all emails on the school network are monitored.
- Will be given a structured education programme that makes them aware of the dangers of and good practices associated with the use of email (see 'Education-Pupils').
- Should use only the school email services to communicate with others when in school.
- Must follow the school rules when sending emails.

Staff:

- Staff should not use their school email address for personal or business use.
- Will be made aware that their emails may be monitored.
- School email addresses are the preferred email address for professional business.
- Any emails sent must be professional in tone and content (for further details, see 'Professional Standards for Staff Communication' section). Personal emails should not be used to contact pupils & parents.

Blogs/ Wiki pages

These may be used to support Computing lessons and other curriculum areas. To ensure the safety of users staff will ensure that:

- Only educational, whole class blog websites are used and that these are password protected.
- Full names of the children in the class will not be used
- Children understand how to communicate respectfully online; any comments made by children (or other users) will not be published until they have been approved by members of staff.
- The use of images complies with school policy (see 'Use of digital and video image' section of this policy).

Video Conferencing

At times the School may use video conferencing to support learning in the classroom, for example to communicate with guest speakers or to practise foreign languages.

At Whitstone School we:

- Only use approved or checked webcam sites, such as Skype Education.
- Ensure children will only take part in whole class video conferencing activities, which are supervised and organised by members of staff.
- Seek parental permission before allowing children to take part in video conferencing.
- Ensure all Video conferencing equipment in classrooms is switched off when not in use and not set to auto answer.
- Will not put Videoconferencing contact information on the school website.
- Only give unique log on and password details for the educational videoconferencing services to members of staff.
- Only use accounts created in the name of the school.
- Only key administrators have access to videoconferencing administration areas.
- Carryout appropriate checks on any guest speakers.

Use of web-based publication tools

Website (and other public facing communications)

Our school website (whitstone.cornwall.sch.uk/) is used for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content:

- Uploading of information is restricted. Only members of staff, who have received training from the Online-Safety Co-ordinator, may adapt school websites.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Personal information should not be posted on the school website;
- Only pupil's first names are used on the website, and only then when necessary (these must not be put with photos);
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images (for further information see 'Use of digital and video images' section);
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- When parents make comments on the school's social media pages, they must not give their child's name (by doing this they will often reveal their child's first and second name, thereby breaking the school's e-safety rules). If this occurs, members of staff will remove comments and remind parents of our 'house rules'.
- If members of the school community encounter inappropriate comments on the school's social media pages, they should report them to the headteacher and follow the school's policy on cyberbullying.
- Written permission from parents or carers will be obtained before photographs/ videos of pupils are published on the school website (these forms are renewed on an annual basis).
- New communication platforms can only be set up following the headteacher's permission.

Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf.) Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, website etc.) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

When using the internet for personal use staff should ensure that:

- No reference should be made in social media to students / 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 are not 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.

Further information on how staff can protect their professional identify online can be found on the NSPCC website and in, 'The Teachers Standards,' 2012.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / 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/ videos on the internet. Such images/ vidoes may provide avenues for cyberbullying 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:

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be captured using school equipment. No images should be used for personal, illegal or business use.
- Care should be taken when taking digital / video images 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 permission.
- With permission from the headteacher, parent/carers may take digital/ video images of pupils at school events. However, they will be asked not to share these on public platforms without permission (Facebook etc). Parents will be reminded of this at such events.

Mobile Devices

All visitors, parents and governors to the school will be made aware of the school's mobile devices and image policies on arrival at Whitstone C.P. School, and will be expected to follow them.

Staff:

Members of staff will ensure that:

•Personal mobile devices are stored securely, away from the view of pupils;

•Any personal mobile devices are password protected;

•They do not use personal mobile devices during lesson time;

•Personal mobile devices are used in areas away from pupils, such as the office or staff room.

•They follow the school's image policy, and not use their own personal devices to take photographs or videos of children.

Trips

During trips, mobile phones provide a useful way for members of staff to stay in contact with one another and report emergencies. Whenever possible, staff should use the school mobile on trips and must always follow the critical incident procedure.

Parents/ volunteers/ governors:
When working in classrooms parents and carers will be asked to:
•Ensure that they do not use personal mobile devices in the classrooms/ or playgrounds.
•Make sure that devices are switched off/ or turned to silent.

During school events, such as plays, parents/ carers will be allowed to use mobile devices. However, they must follow the school policy on images and not sure these on social media platforms.

Pupils:
Pupils may only bring phones or mobile devices into school with the permission of the headteacher. These should be handed in to a member of staff and be clearly labelled. Members of staff will store these securely.

Where pupils' mobile devices are used inappropriately, they may be confiscated and images/ videos may be deleted. When this occurs, staff will follow the school's behaviour and anti-bullying policy.

The school accepts no responsibility for the lost or damage of personal devices.

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school / network is as safe and secure as is reasonably possible

Filtering and Monitoring

At Whitstone C.P. School access to the internet is filtered for all users. The school filter is provided by Netsweeper and maintained by NCi. The filtering system complies with Ofsted's requirements.

Internet access is filtered for all users. Illegal content (eg. 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. The school filtering system blocks both inappropriate and illegal material. The Internet filtering system has been designed to ensure that children are safe from terrorist and extremist material when accessing the internet.

However, staff at Whitstone C.P. School understand that on rare occassions the school filter may not prevent users from accessing all inappropriate/ illegal material. Therefore children are not allowed to use ICT without the supervision of an adult. Members of staff and pupils should report any failures in the school's filtering system to the E-Safety Co-ordinator and NCi.

The school / academy has provided enhanced / differentiated user-level, with differing profiles for staff and children. Sometimes members of staff may wish to access websites that have been blocked, for educational purposes. For example, when accessing videos that they wish to share with children. When this is case they may request for websites to be unblocked on staff profiles. Certain filtering categories cannot be unblocked by members of staff (see list provided by NCi).

All users are aware that the ICT technicians from NCi, monitor the information accessed by members of the school community. NCi sends regular updates to the Computing Co-ordinator on sites that have been accessed by members of Whitstone C.P. School.

For further information on the school's filtering system, the school's E-Safety Co-ordinator or NCi technicians should be contacted.

Technical Systems

- There will be regular reviews and audits of the safety and security of school's technical systems which will be carried out by NCi;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users have clearly defined access rights to school technical systems and devices.
- The headteacher has access to administrator rights.
- Appropriate security measures have been put in place by NCi 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 school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- Only members of staff may download files and when this occurs they must be scanned for viruses;
- Members of staff must inform NCi and seek permission from the headteacher before installing new software. Where there is a charge for software, Mrs Slade must also be informed.
- A list of school software is kept by NCi.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices (see data protection section below)

Data Protection

Personal data will be recorded, processed, transferred and made available according to

The Data Protection Act 1998 which states that personal data must be:

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

To protect data staff must ensure that they:

- take care to ensure the safe keeping of personal data at all times, 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.
- Change passwords on a regular basis and ensure that they do not them.
- transfer data using encryption and secure password protected devices (passwords chosen should be strong. Eg. Using characters, numbers and capital letters).

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 (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Further information can be found in the school's Data Protection Policy.

Training

At Whitstone C.P. School we recognise that technology is constantly changing. The Online Safety Co-ordinator provides staff with regular training and updates, through INSET sessions, as well as through regular Online Safety newsletters.
All staff have received training in child protection and are aware of their responsibilities with regard to the 'PREVENT' duty.

Futher information is also available in the school's safeguarding policies.

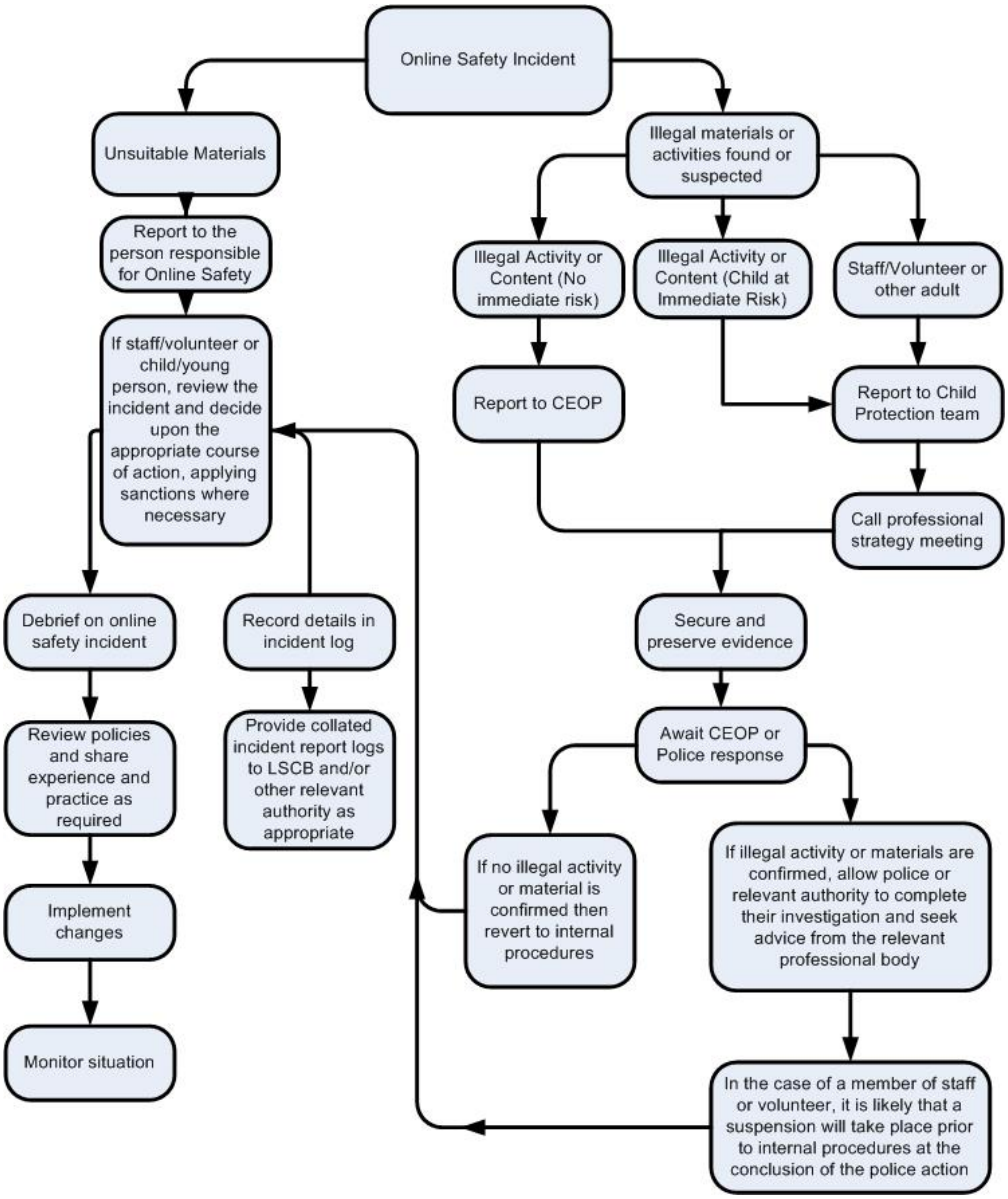
Responding to incidents of misuse

This 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.

SWGfL BOOST (South West Grid for Learning) includes a comprehensive and interactive 'Incident Management Tool' that staff will be able to use when managing and reporting E-Safety incidents (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

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 (following page) for responding to online safety incidents 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:

- When an Online Safety incident occurs the Online Safety Co-ordinator, headteacher and Online Safety governor will become involved this process. This is vital to protect individuals if accusations are subsequently reported.

- Procedures will be followed 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. The same computer will be used for the duration of the process.
- 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).
- The url of any site containing the alleged misuse should be recorded and the nature of the content causing concern should be described. 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 (as relevant).
- 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.**

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.

Sanctions for pupils;

It is more likely that the school / academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

When pupils do not adhere to the school's Acceptable Usage Policy, members of staff may follow behaviour and anti-bullying policies. If required, staff may also follow safe-guarding procedures and/ or work with outside agencies. Any E-Safety incidents should also be logged in the Online Safety log book (in the headteacher's office) and reported to the headteacher and Online Safety Co-ordinator.

Policy to be reviewed: October 2018 (or sooner, if required.)

This policy has been produced with support from the South West Grid for Learning: http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Key Stage 1 pupil agreement

I will ask for permission from a member of staff before using the computers in school.

I will ask for permission from a member of staff before using the Internet.

I will only use the computers/ ipads in school for school work or homework.

I will not bring in and use any portable device (i.e.USB stick) from outside school without asking a member of staff.

I will tell a member of staff if I see anything unpleasant or that I am unhappy with on the computer.

I will always be kind to others when working online and on the computer.

I know that school staff may check the Internet sites I visit.

I know the school may check my computer files.

I understand that if I deliberately break these rules I could be stopped from using the school's computers/ ipads.

Key Stage 2 pupil agreement

I will ask for permission from a member of staff before using the computers, ipads and internet in school.

I will only use the computers/ ipads in school for school work or homework.

I know that school staff may check the Internet sites I visit.

I will not bring in and use any portable device (i.e.USB stick) from outside school without asking a member of staff.

I will not use my own mobile devices in school (tablets, phones
, cameras etc), unless I have permission.

I will ask for permission before taking and using photos.

I will tell a member of staff if I see anything unpleasant or that I am unhappy with on the computer.

I know about 'stranger danger' and will not share personal information when working online, such as my telephone number, address etc.

I understand that my passwords should be kept private.

I will always be polite to others when working online.

I will not damage anyone else's work.

I will not download programs or apps onto the school computers or Ipads.

I will not alter computer settings (eg. screen savers etc).

I know the school may check my computer files.

I understand that if I deliberately break these rules I could be stopped from using the school's computers/ ipads.

DATE APPROVED:- September 2019

DATE OF NEXT REVIEW:- September 2020