E-Safety Policy

Schedule for Development/Monitoring/Review

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Scope of the Policy

This policy applies to all members of Sandwell Valley School and Sandwell Community Care Trust Training (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of SCT Training ICT systems, both in and out of the centre.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students 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 e-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.

Sandwell Valley School and Sandwell Community Care Trust Training will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Sandwell Valley School and Sandwell Community Care Trust Training.

Governors:

Governors are responsible for the approval of the E-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.

Principal of Centre and Senior Leaders:

The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community

The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local

Authority HR / other relevant body disciplinary procedures).

The Principal/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the E- Safety Co-ordinator/ Designated Senior Person.

E-Safety Coordinator/Designated Senior Person:
leads on e-safety issues
takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
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 the Local Authority/relevant body
o liaises with school technical staff
o liaises with school technical staff
o   receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
o attends relevant meeting/committee of Governors
o reports regularly to Senior Leadership Team

Network Manager:
The Network Manager is responsible for ensuring:
that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
that the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
that the use of the network/internet/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal/ E-Safety Coordinator/Designated Senior Leader for investigation/action/sanction.
that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

they report any suspected misuse or problem to the Principal/E-Safety Coordinator/Designated Senior Person for investigation/action/sanction.

all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.

e-safety issues are embedded in all aspects of the curriculum and other activities.

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

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 students 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

Students:

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 E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. 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.

access to parents' sections of the website and on-line student records.

their children's personal devices in the school (where this is allowed)

Community Users:

Community Users who access school systems/website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e- safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned e-safety curriculum should be provided as part of ICT/PHSE/other lessons and should be regularly revisited.

Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Staff should act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that students 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.

Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents/carers:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

  Curriculum activities
  Letters, web site
  Parents/Carers evenings/sessions

Education – The Wider Community:

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

Providing family learning courses in use of new digital technologies, digital literacy and e-safety

The school website will provide e-safety information for the wider community

Education & Training – Staff/Volunteers:

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

A planned programme of formal e-safety training will be made available to staff.
This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

The E-Safety Coordinator/Designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.

This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

The E-Safety Coordinator will provide advice/guidance/training to individuals as required.
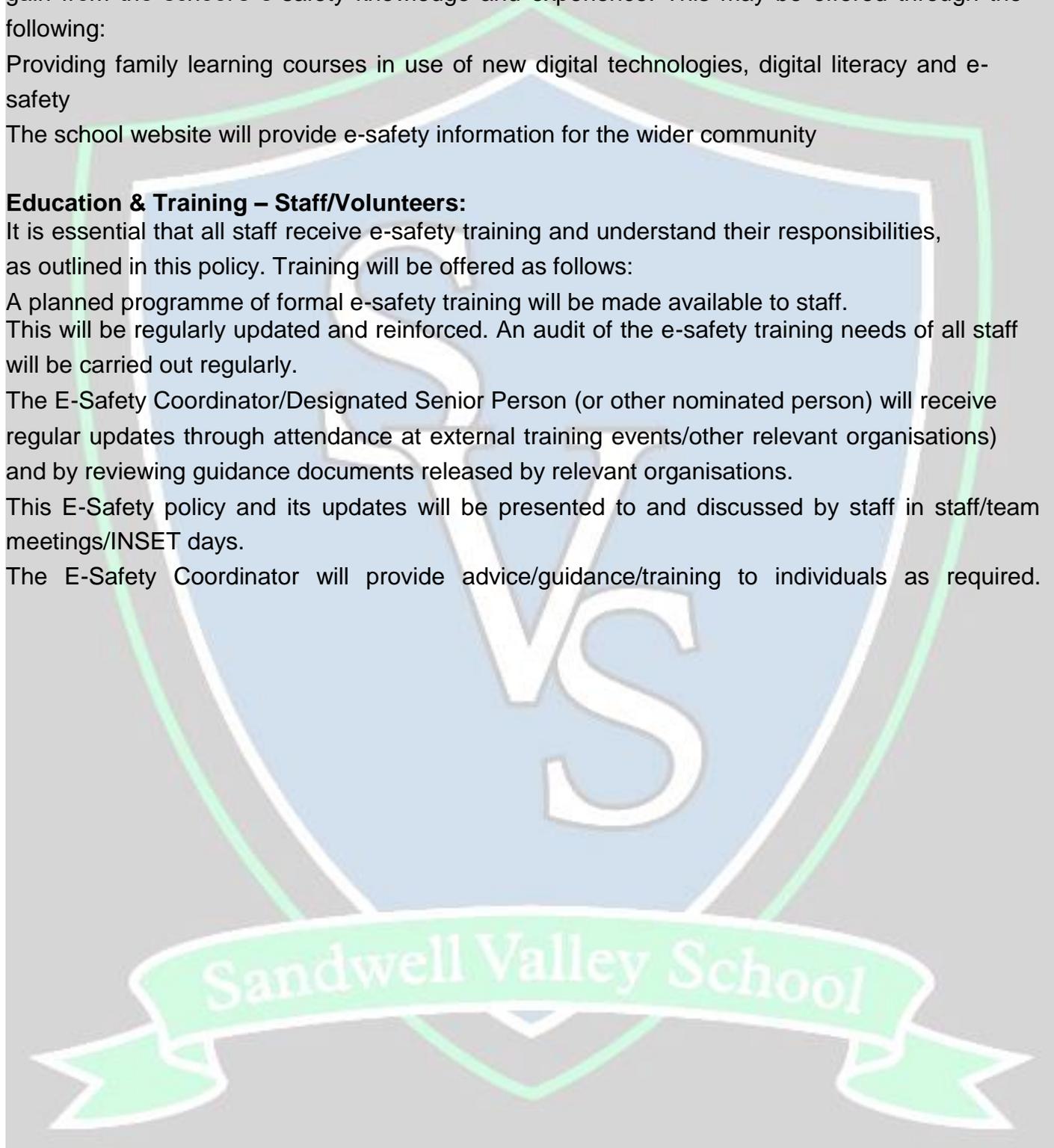
Training – Governors:

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

Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.

Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure/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 e- safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

There will be regular reviews and audits of the safety and security of school technical systems

All users will have clearly defined access rights to school systems and devices.

All users will be provided with a username and secure password. Users are responsible for the security of their username and password.

The school has provided enhanced/differentiated user-level filtering

An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.

An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.

Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the IT department.

Users may use the following types of removable media for the purposes detailed:

o   CD/DVD – Playing original video material, original music and viewing

data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.

° USB Media (memory sticks) – this type of media can be used on
school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.

O Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images 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:

When using digital images, staff should inform and educate students 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 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/carers comment on any activities involving other students in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of students are published on the school website.

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

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.

Staff must ensure that they:

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

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

Transfer data using encryption and secure password protected devices.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice:

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel

uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

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

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

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

Social Media - Protecting Professional Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

Training to include: 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 students, 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.
The school's use of social media for professional purposes will be checked regularly.

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
All staff should receive a copy of the E-Safety Policy.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Principal/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

School should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and
'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use
Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:
Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

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 (see "In the Event of Inappropriate Use" above). See flow chart on the next page.

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 (below and appendix) 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:
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:
o Internal response or discipline procedures.

o   Involvement by Local Authority or national/local organisation (as relevant). o Police involvement and/or action.

o   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.
incidents of 'grooming' behaviour.
the sending of obscene materials to a child.
adult material which potentially breaches the Obscene
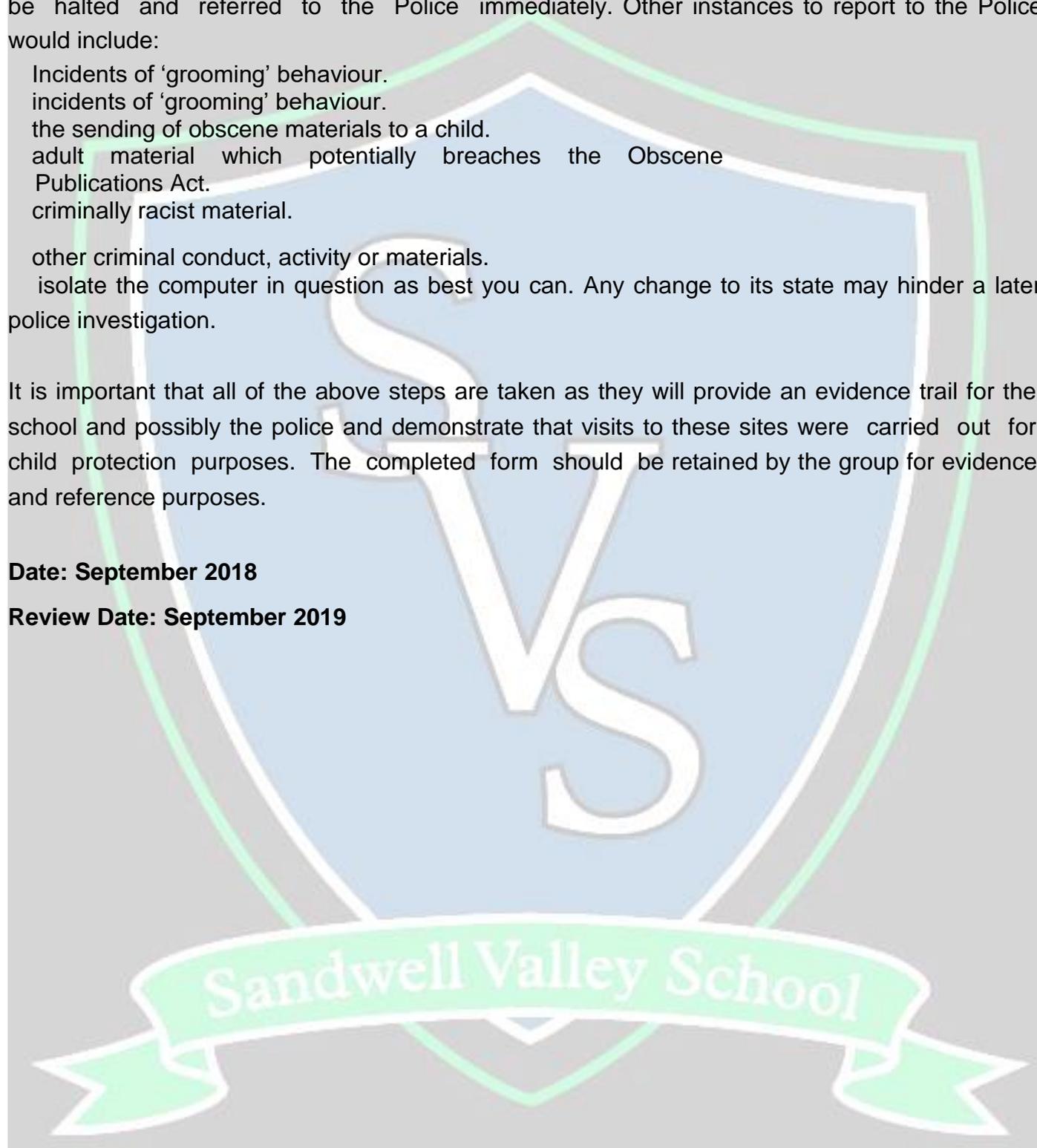 Publications Act.
criminally racist material.

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.

Date: September 2018

Review Date: September 2019