Sandford St. Martin's
PRIMARY SCHOOL

E-Safety Policy and Procedure 2023-24

Our mission statement: Learn Love Laugh

Safeguarding

If there are any Safeguarding issues that arise from the implementation of this policy, then they should be dealt with in accordance with the School's Safeguarding policy. Any safeguarding concerns should be referred directly to the School by telephone or in person for the attention of the Designated Safeguarding Lead along with any concerns relating to the Prevent Strategy.

Equality

This policy should be read in conjunction with the School's Equality Policy. The general equality duty requires that, in the exercise of their functions, schools must have due regard to the need to eliminate unlawful discrimination, harassment, victimisation and other conduct prohibited by the Equality Act 2010. This school endeavours to advance equality of opportunity and foster good relations for all.

Background

This E-safety policy is designed to help ensure the safe and appropriate use of new technologies and the internet; both of which have become integral to the lives of children and young people in today's society, within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people have an entitlement to safe internet access at all times. However, the use of these new technologies and the internet can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and as such this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies, Keeping Children Safe in Education and the Prevent Strategy).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks appropriately.

1. Monitoring and Review of this Policy

This E-safety Policy has been developed by a working group made up of:
- School E-safety Lead (Computing Lead) and Headteacher (DDSL)
- Deputy Headteacher and Designated Safeguarding Lead
- Safeguarding and E-safety Governors
- DSSL staff member with E-safety experience

2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital information systems, both in and out of school.
The school will deal with E-safety incidents in the same way as associated behaviour and bullying incident and will, where it becomes aware, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

3. Schedule for Development / Monitoring / Review

This E-safety policy was approved by the Governing Body.

The implementation of this E-safety policy will be monitored by the E-safety lead. Monitoring will take place continuously.

The Governing Body will receive a report on the implementation of the E-safety policy generated by the Computing Lead and SLT (which will include anonymous details of online safety incidents) at each Full Governing Body meeting.

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 online safety or incidents that have taken place.

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

- SWGfL
- Parents / carers
- Staff
- Police: Safer Communities team
- Police: where a criminal offence has been committed

4. Roles and Responsibilities

4.1 Governors

Governors are responsible for the approval and adoption of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-safety Governor. The role of the E-safety Governor will include:

- regular meetings with the E-Safety Lead (also a Deputy Designated Safeguarding Lead) to discuss any E-safety incident log entries, filtering issues etc. *(if the Lead is not the Headteacher).*
- reporting to the Governing Body as required

4.2 Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including E-safety) of members of the school community
- The Headteacher and Deputy Headteacher 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 online safety incidents "Responding to incidents of misuse" in Section 13).
- The Headteacher / Senior Leadership Team (SLT) are responsible for ensuring that the E-safety Lead and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues. *(if the Lead is not part the Headteacher).*
- The Headteacher/SLT 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, all issues will be brought to the attention of the Deputy Headteacher.
- The Senior Leadership Team will receive monitoring updates from the E- safety Co-ordinator (if the Lead is not already part of the SLT).

4.3 E-safety Co-ordinator (Head of Computing) – *if not the Headteacher*

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body (when necessary)
- receives reports of online safety incidents and creates a log of incidents to inform future E-safety developments (stored on the Staff drive: ICT/online safety incidents reporting log.doc)
- meets with the Deputy Headteacher and / or online safety Governor to discuss any current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors, as requested
- liaises regularly with the Deputy Headteacher and Assistant Headteacher
- liaises with Senior Staff/DSLs to decide how E-safety incidents will be dealt with and whether further investigation / action / sanctions are required.

4.4 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 have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-safety Lead /Headteacher
- all digital communications with students/pupils/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 school activities
- pupils understand and follow the school E-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT/computing activity in lessons, extra-curricular and extended school activities
- they offer suitable support and understanding for victims/distressed persons/viewers of any inappropriate materials
- they are aware of E-safety issues related to the use of mobile phones, cameras, and hand-held devices, and that they monitor their use and implement current school policies with regard to these devices. In lessons where internet use is pre-planned consideration should be made of guiding pupils 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
- they are aware of the E-safety issues that are related to on-line communication that can take place during on-line gaming

4.5 Designated Safeguarding Lead and DDSLs

should be trained in E-safety issues and be aware of the potential for serious child protection issues to arise from:

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

4.6 Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (at age appropriate level as delivered in the curriculum)
- 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 school policies on the use of mobile phones, digital cameras and hand-held devices.
- should know and understand school policies on the taking / use of images, including their use as part of our anti online-bullying and anti sexting.
- should understand the importance of adopting good E-safety practice when using digital technologies out of school

4.7 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will help parents understand these issues through parents' evenings, newsletters, letters, website / local online safety campaigns / literature.

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
- access to parents' sections of the website / and on-line pupil records
- their children's personal devices in the school (where this has been allowed)

Parents and carers will be responsible for:

- endorsing the Pupil Acceptable Use Policy
- accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

5. <u>Curriculum</u>

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages in the use of ICT across the curriculum:

- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to search the internet independently in lessons, e.g. using search engines, 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, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (SWGfL) 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.
- pupils 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
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- In planning the online safety curriculum, teachers may wish to refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

6. Education & Training

6.1 Parents/carers

Parents and carers may well 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 through:

- Letters, including the school newsletter
- The school website online safety page http://www.sandfordprimary.dorset.sch.uk/online safety-information/
- Parents evenings and specific online safety information evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g.:
  - Safer Schools & Community Team Newsletters;
  - www.swgfl.org.uk
  - www.saferinternet.org.uk/
  - http://www.childnet.com/parents-and-carers (see Section 16 below for further links / resources)
  - Thinkuknow - home

6.2 Staff

All staff should receive E-safety current updates and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements (signed agreement to be filed in staff records).
- The E-safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL / other relevant organisations), by signing up for regular email updates or 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 meetings or during Inset days.
- The E-safety Lead will provide advice / guidance / training to individuals as required.

6.3 Governors

Governors will keep informed by checking the regular E-safety updates on school website; take part in E-safety training / awareness session, either by completing an on-line course or participation in school training / information sessions for staff, parents or governors.

7. Technical – infrastructure/equipment, filtering and monitoring

Internet access is filtered for all users. Illegal content (including child sexual abuse images) is filtered by the SWGfL filtering service. Content lists are regularly updated. Requests for filtering changes are to be made to the E-safety Lead (Computing Lead).
Any actual / potential technical incident / security breach should be reported to the E- safety Lead (Computing Lead) or the Deputy/Headteacher.

8. Bring Your Own Device (BYOD)

Pupils at the School are not currently permitted to bring devices into school unless there is a recognised educational or physical need e.g. use of a word processor in English for a child with dyslexia. Permission should be sought from the Headteacher. Devices are brought into school at the risk of the owner. Staff may bring in personal devices but at their own risk.

- All users may access their devices in accordance with the school Acceptable Use Agreement
- The device must include up-to-date virus and malware checking software
- All network systems are secure and access for users is differentiated
- Where possible, these devices will be covered by the school's normal filtering systems, while being used on the premises (excludes 3G, 4G)
- The school adheres to the GDPR principles
- Mobile phones are handed into the office and not permitted to be carried by pupils in the school day

9. Use of digital and video images - Photographic, Video

Staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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.
- Staff 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.
- Parents are advised not to take images / videos without permission. To respect everyone's privacy and in some cases protection, images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils.
- 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 their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

10. Data Protection/GDPR

When personal data is stored on any portable computer system, memory stick, or any other removable media or device (including phones), the school strongly recommends that staff:

- 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
- ensure that they are properly "logged-off" at the end of any session or 'remote' session
- transfer data using encryption and secure password protected devices where possible
- access sensitive / personal data from home using their 'remote' login rather than copying data onto unprotected memory sticks or external hard drives
- securely delete data from any device once it has been transferred or its use is complete
- report any loss or theft of a removable / portable device containing sensitive / personal data to the Computing Lead as soon as possible.

11. Unsuitable / inappropriate activities

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution.

The school believes that the activities referred to in the following section are inappropriate in a school context and that users should not engage in the activities as defined below in / or outside the school when using school equipment or systems. The school policy therefore prohibits such usage:

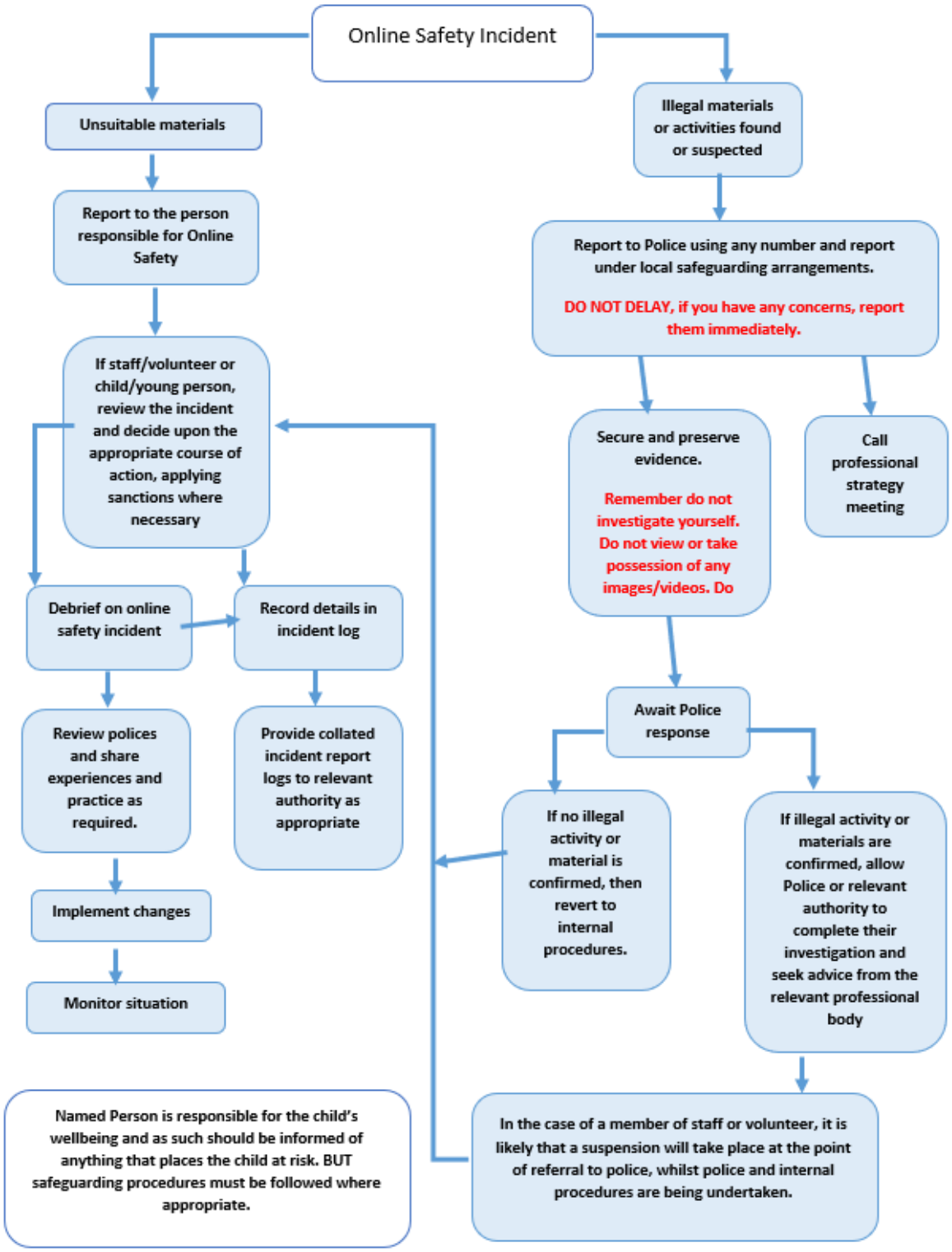
- Promotion of any kind of discrimination
- Accessing or sharing information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming (non-educational)
- On-line gambling

12. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the mis-use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

12.1 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, **report immediately to the police** and refer to the right-hand side of the Flowchart (below and Section 14) for responding to online safety incidents.



12.2 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:

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- 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 (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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

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 safeguarding purposes. The completed set of records should be retained by the group for evidence and reference purposes.

Reporting Incidents involving the use of technology

Schools should pursue appropriate lines of intervention and protection following any incident. This may involve contacting the Police and/or social care. See the Pan-Dorset Multi Agency Safeguarding Procedures for more information.

The Dorset Safe Schools and Communities Team (SSCT) operates the Dorset Police Triage service with the aim of responding more effectively to school and youth internet incidents. Reports to the police relating to youth internet safety incidents will be referred to the SSCT to manage. The types of incidents that may be dealt with via this route include: Bullying (including low-level school assaults), experimental sexting, other E-Safety incidents involving only young people and that are not of a serious nature. The aim of this initiative is to support young people, parents, carers and their schools to deal with these incidents appropriately, proportionately and effectively.

Schools may refer these types of incidents directly to the SSCT on 01202 222844 or **ssct@dorset.pnn.police.uk**. Other organisations should refer any concerns to the MASH (Safeguarding Referral Unit) for Dorset Police on 01202 22229.

13 School Actions & Sanctions

It is more likely that the school 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. It is intended that incidents of misuse and the action/sanction selected in each case will be dealt with through normal behaviour / disciplinary procedures as follows:

13.1 Pupils Incidents

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Unauthorised use of non-educational sites during lessons
- Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device
- Unauthorised / inappropriate use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

13.2 Actions/Sanctions for Pupil Incidents (applied depending on nature of incident)

Action/sanction selected from the following:

- Refer to class teacher
- Refer to Key Stage Lead (AHT/DHT)
- Refer to Headteacher
- Refer to Police
- Refer to technical support staff for action re filtering / security etc.
- Inform parents / carers
- Removal of network / internet access rights
- Warning
- Further sanctions in line with school behaviour policy

13.3 Staff Incidents

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Inappropriate personal use of the internet / social media / personal email

- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

13.4 Actions/Sanctions for Staff Incidents (applied depending on nature of incident and subject to disciplinary policy and procedure)

Action/sanction selected from the following:

- Refer to line manager
- Refer to Headteacher
- Refer to Local Authority / HR
- Refer to police
- Refer to Technical Support Staff for action re filtering etc
- Warning
- Suspension
- Disciplinary action

14 Useful online safety Resources (General Resource list provided by SWGfL)

- The Dorset Police SSCT (Safe School and Communities Team) publish useful online safety newsletters available here: Stop Think Dorset parents online safety newsletters.
- Parenting in the Digital Age (or PitDA for short): Parenting in the Digital Age Website
- Ofcom's guidelines on safe use of the internet: Ofcom
- DASP online safety Web Page http://www.dasp.org.uk/e-safety.htm
- Child Exploitation and Online Protection Centre http://www.ceop.gov.uk/
- Thinkuknow http://www.thinkuknow.co.uk/
- Childnet International http://www.childnet.com
- Safer Internet Day http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- Get Safe Online http://www.getsafeonline.org
- Cyberbullying.org - http://www.cyberbullying.org/
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- https://www.gov.uk/government/publications/education-for-a-connected-world

Example incident log sheet attached.

SANDFORD ST MARTIN'S CE (VA) PRIMARY SCHOOL

E-safety Policy	
Date adopted: 25 May 2022	**Version: 4.0**
Last Reviewed: April 2023	**Review Cycle: Annual**
Revision Ref:	**24 May 2024**
Author/Owner:	**E-safety Lead/E-safety Governor/DSL/Headteachers/FRC/SAC**
Policy Type:	**Safeguarding**

Online safety incident report form

This form should be passed to the school online safety officer and Senior Leadership as appropriate

Details of incident

Date incident happened:

Time:

Name of person reporting incident: (If not reported, how was the incident identified?)

Where did the incident occur?

□ In school □ Outside school

Who was involved in the incident?

□ child/young person □ staff member □ other (please specify

Type of incident:

□ bullying or harassment (cyber bullying)

□

□ deliberately bypassing security or access

□ hacking or virus propagation

□ racist, sexist, homophobic religious hate material

□ terrorist material

□ drug/bomb making material

□ child abuse images

□ on-line gambling

□ soft core pornographic material

□ illegal hard-core pornographic material

□ other (please specify)

Description of incident

Nature of incident

Deliberate access □

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Could the incident be considered as;

□ harassment □ grooming □ cyber bullying □ breach of AUP

Accidental access □

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Action taken

□ **Staff**

□ incident reported to head teacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to Internet Watch Foundation

□ incident reported to IT

□ disciplinary action to be taken

□ online safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to head teacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to social networking site

□ incident reported to IT

□ child's parents informed

□ disciplinary action to be taken

□ child/young person debriefed

□ online safety policy to be reviewed/amended

Outcome of incident/investigation