Sunninghill
PREP SCHOOL DORCHESTER

# E-Safety Policy

This policy incorporates the following policies:

- Technical Infrastructure
- Mobile Technologies and BYOD
- Social Media - Protecting Professional Identity

Nov 2018

360safe the e-safety self review tool

SOUTH WEST GRID FOR LEARNING

digital Friendly WiFi The Safe Certification Standard for Public WiFi

# Who to contact for help and advice

| | |
|---|---|
| **If a child is at immediate risk, dial 999.**<br><br>**Should serious e-safety incidents take place, the following external persons/ agencies can be contacted:**<br><br>**CEOP and IWF websites can be used to confidentially report online sexual abuse / criminal content.** | **SSCT - Safe Schools team, Dorset Police**<br>Tel: 01202 222844<br>Email: ssct@dorset.pnn.police.uk<br>Web: http://www.stopthinkdorset.co.uk/<br><br>**MASH (Multi-Agency Safeguarding Hub)**<br>Tel: 01202 228866<br>Email: MASH@dorsetcc.gov.uk<br><br>**Dorset Safeguarding and Standards Team** Tel: 01305 221122<br><br>**Cyberbullying or digital safety concern?**<br>**Contact the SWGfL professionals online safety helpline**<br>Tel: 0344 381 4772<br>email: helpline@saferinternet.org.uk<br><br>**Online reporting tools:**<br>CEOP Child Exploitation and Online Protection command<br>or<br>IWF Internet Watch Foundation |

# Contents

# Introduction

Sunninghill embraces technology and the advances in this area when used to support learning. Whilst the emphasis in education should be on the positive use of the Internet, there is a need to address the dangers and raise awareness of potential abuses of this technology, especially in light of recent high-profile cases in the media, including strong evidence of online strategies being employed to radicalise young people.

We are committed to safeguarding the welfare of all pupils. Sunninghill is committed to providing a safe, caring and friendly environment for all staff and pupils. We wish to involve the appropriate use of the Internet, and we actively invite the participation of parents to help us to do this.

Bullying of any kind is unacceptable.

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.

This policy is written with due regard to Keeping Children Safe in Education, 2018 and DFE Guidance July 2017: *Preventing and Tackling Bullying*, *Cyber bullying: advice for headteachers and school staff*. It should be read in conjunction with other school policies: Safeguarding (Child Protection policy); Mobile Phone Use, Behaviour Policy and Anti-bullying. (NB. E-Safety is increasingly referred to as Online Safety.)

**Some of the e-safety dangers children 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
- 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, 'addiction' which may impact on the social and emotional development and learning of the young person.
- Cyber-bullying

## What is Cyber-bullying?

Cyber-bullying can be defined as the deliberate use of ICT, particularly the Internet, mobile phones and digital devices such as cameras, tablet devices, and smartphones, to upset someone else. It may take the form of abuse of an individual due, for example, to their status, physical qualities, characteristics, race, religion, sexual orientation, class or the activities with which they have been involved. Bullying by text, e-mail, phone call, or social media often leaves no physical scars, but can be highly intrusive and hurtful. We therefore take cyber-bullying, like all bullying, very seriously.
All of the following actions are classed as cyber-bullying, and will be dealt with accordingly by the School:

- Sending threatening or abusive messages
- Creating and sharing embarrassing videos
- 'Trolling' – the sending of menacing or upsetting messages on social networks, chat rooms or online games, whether this is from a known or unknown person
- Excluding someone from online games, activities or friendship groups
- Setting up hate sites or groups about a particular person
- Encouraging young people to self-harm
- Voting for or against someone in an abusive poll
- Creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

This peer-on-peer abuse will not be tolerated, and never be accepted as "banter" or "part of growing up". Victims of cyberbullying and/or sexting will receive full pastoral support; those responsible will be subject to the School's sanctions policy, and liaison with Social Care and/or the Police will be considered.

## Monitoring and Review of this Policy

This E-Safety Policy has been developed with input from:

- School E-Safety Champion: Nancy Sewed (Deputy Head Academic): nsewed@sunninghill.dorset.sch.uk
- DSL: Nikki Carr ncarr@sunninghill.dorset.sch.uk
- Deputy Head Pastoral: Ian Stazicker istazicker@sunninghill.dorset.sch.uk
- ICT Technical support: Flatrock Systems Ltd (recently merged with DDBi)
- Safeguarding Governor: Stephanie Dean

Child views are taken into consideration via class discussions in computing lessons and feedback from our E-Safety Group.

| | |
|---|---|
| The implementation of this E-Safety Policy will be monitored by the: | School E-Safety Champion, DSL, SLT |
| Monitoring will take place at regular intervals: | Annually |
| 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 or new threats to e-safety or incidents that have taken place. Next anticipated review date: | Nov 2019 |

The school can monitor the impact of the policy using:

- Logs of reported incidents
- South West Grid for Learning(SWGfL) monitoring logs of internet activity
- Feedback from teaching and learning support staff and pupils.
- Surveys of pupils

## Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/guardians, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Heads 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 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

We will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

# Roles and Responsibilities

## Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. Our Safeguarding Governor is **Stephanie Dean.**

The role of the Safeguarding Governor includes:

- regular meetings with the DSL and E-Safety Champion to discuss any e-safety incident log entries, filtering issues etc.
- incidence to be logged and included in the annual safeguarding report.

## Head teacher and Senior Leaders:

- The Head has a duty of care for ensuring the safety of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Champion.
- The Head and Deputy Head (Pastoral) are to 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 "Responding to incidents of misuse" in the Appendix.
- The Head / Senior Leadership Team (SLT) are responsible for ensuring that the E-Safety Champion and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues.
- To 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 Head (Pastoral).
- The Senior Leadership Team will receive monitoring updates from the E-Safety Champion.

## E-Safety Champion:

- 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
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (stored on the Staff drive)
- meets with the DSL / Deputy Head (Pastoral) and / or Safeguarding Governor to discuss any current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors, as requested
- reports to the Senior Leadership Team
- liaises with the DSL / Deputy Head (Pastoral) or Head to decide how e-safety incidents will be dealt with.
- Conducts a regular school review to assess provision using the 360 degree Online Safety Self Review tool

## Network Manager/Technical staff Responsibilities

Network support is provided by an external company: Flatrock Systems Ltd 01305 262306 (also known as DDBi: 08450 041184)

The Network Manager and Head of Computing (Nancy Sewed) are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and guidance
  that users may only access the school's networks through their password protected account
- SWGfL is informed of issues relating to the filtering applied by the Grid
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

## Teaching and Support Staff Responsibilities

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and have read the current school E-Safety Policy
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Champion, SLT or Head for appropriate investigation/action/sanction
- all digital communications with pupils must be on a professional level and carried out using official school systems where across 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 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. Any unsuitable material that is found in internet searches should be reported to the e-safety champion, Head or SLT.

**'Safe search settings' should be manually enabled by staff when using search engines e.g. Google and YouTube.**

## Designated Safeguarding Lead Responsibilities

The DSL has overall responsibility for e-safety, and is trained in e-safety issues and aware of the potential for serious child protection / safeguarding issues arising from:

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

## E-Safety Group

The school Pupil Voice group is made up a member of staff and two representatives from each year group. This group also acts as the E-Safety Group and assist the E-Safety Champion by:

- commenting on e-safety education to ensure relevance
- educating groups e.g. by giving assemblies
- sharing their classmates experiences and concerns relating to e-safety

## Pupils:

- Forms 3 – 8 are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (AUP). They will be expected to sign the AUP before being given access to school systems (parents/guardians can sign on behalf of the younger pupils).

- new pupils sign a copy of the AUP on entry to the school. Pupils are reminded of the contents of the policy annually and sign a pre-printed page in their school diaries.
- 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 and Carers Responsibilities

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe way.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy on entry to the school
- accessing the school website/parent portal (3sys) in accordance with the relevant school Acceptable Use Policy.

We asks parents to:

- Support the School in its E-Safety Policy.
- Try to know their child's online friends as they know their actual friends.
- Ensure that computer use at home is not excessive, and is appropriately monitored.

Should parents have any concerns over, or wish to seek guidance on any aspect of e-safety, they are encouraged to contact the relevant E-Safety Champion, DSL or Deputy Head (Pastoral).
Should parents have concerns that a pupil has been subjected to attempts at sexual grooming, radicalisation, or other inappropriate online contact, they should contact the School immediately. The Designated Safeguarding Lead will, where appropriate, liaise with outside agencies, in particular CEOP (Child Exploitation and Online Protection), and SSCT (Safe Schools and Communities Team), as well as Local Safeguarding Children Boards where appropriate

## Policy Statements

### Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. E-safety should therefore be a focus in *all* areas of the curriculum and staff should reinforce e-safety messages across the curriculum.
Discrete E-Safety education is provided in the following ways:

- A planned e-safety programme is provided as part of computing and some PSHCE lessons. The school scheme of work is updated annually to include best practise but based on the scheme from SWGfL http://www.digital-literacy.org.uk/Home.aspx
- Key e-safety messages are reinforced in assemblies where possible e.g. cyber-bullying
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Pupil will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will 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.

- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- 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 pupils should be guided to sites checked as suitable for their use. Processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils 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 (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. Staff can request that the Head of Computing can temporarily remove those sites from the filtered list for the period of study.

### Education – parents/guardians and the wider community

Many parents and carers have only a limited understanding of e-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 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.

We will provide awareness and regular termly e-safety updates to parents, carers and relatives via:

- Letters, Hermes school newsletters
- The school website e-safety page www.sunninghillprep.co.uk
- Parents evenings
- Online safety messages targeted towards relatives as well aa other parents.
- National campaigns e.g. Safer Internet Day
- Reference to relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

### Education & Training – Staff

All staff receive ongoing e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Agreement (signed agreement to be filed in staff record).
- The e-safety champion will receive regular updates through attendance at external training events (eg from SWGfL / other relevant organisations), by signing up for regular email updates and by reviewing guidance documents released by relevant organisations.
- The E- Safety policy and its updates will be presented to and discussed by staff in staff meetings or during INSET days.
- The e-safety champion will provide advice / guidance / training to individuals as required.
- 'E-safety adviser' newsletters and SSCT newsletters are circulated to all staff and parents on a termly basis.

### Training – Governors

Governors are trained in e-safety along as part of their safeguarding training. This can take different forms:

- by completing an on-line course
- or participation in school training / information sessions / assemblies

## Technical – infrastructure/equipment, filtering and monitoring

1. There will be annual reviews of the safety and security of school technical systems.
2. Where possible, servers, wireless systems and cabling will be securely located and physical access restricted
3. All users will have clearly defined access rights to school technical systems and devices
4. All users (at KS1 and above) will be provided with a username and password by the Head of Computing. Users are responsible for the security of their username and password and will be reminded to change their password periodically.
5. The "administrator" passwords for the school ICT systems, used by the Network Manager must also be available to Bursar
6. Flatrock Systems (also known as DDBi) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
7. Internet access is filtered for all users. Illegal content (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 Head of Computing (Nancy Sewed). Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.
8. Internet activity for all users is logged. The school technical staff may monitor and access the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
9. Any actual / potential technical incident / security breach should be reported to the Head of Computing or Jon Stow at Flatrock.
10. Appropriate security measures (passwords) are in place 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. The school infrastructure and individual workstations are protected by up to date virus software.
11. Guest logins are not allowed. All users will need to request a login from the Head of Computing and sign an AUP before access will be granted.
12. Only administrator logins allow the downloading of executable files and installation of programmes on school devices.
13. The school recommends that personal data concerning staff or pupils is not sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Memory sticks / external hard drives without security measures are not a safe method to transfer sensitive data.
14. Staff may use removable media on school devices but must ensure they maintain up-to-date virus protection on their home device.

## Mobile Technologies including Bring Your Own Device (BYOD)

Pupils are not currently permitted to bring mobile 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 Head in the first instance, and parents are advised to take out insurance in case of loss or damage. Use of 3G /4G on any device is not allowed by pupils (without teacher permission) as this will circumvent the school internet filter.

Staff may bring in personal devices but do so at their own risk. They will not be able to access the school network.

Personal devices owned by pupils, staff or visitors may not be used to take photos or videos in school. Visitors will be informed regarding school requirements when signing in. *See separate school staff Mobile Phone Policy – Main School and Early Years*

- All staff and pupils must access their devices in accordance with the school **Acceptable Use Agreement** (see separate Acceptable Use Policy)
- 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)

- Any device loss, theft, change of ownership of the device is to be reported to the Bursar or Head of Computing.
- Any user leaving the school will follow the processes outlined within the Confirmation of end of contract letter including the removal of all school data
- The school adheres to the Data Protection Act principles

### Sunninghill Guest Network Internet Access

Visitors requiring internet access are to use the guest wireless network SSID: **Sunninghill-Guest.** A disclaimer is displayed when a user first connects to this WiFi network.

## Use of digital and video images – Staff and Pupils

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- 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 / academy events for their own personal use (as such use in 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 pupils 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. It is recommended that the personal equipment of staff is <u>not</u> used for such purposes.
- 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 or videos 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. Work may only be published with their permission.
- Written permission from parents or carers will be sought on entry to the school. Only images of pupils whose parents have given their permission may be used for marketing purposes or published on the school website.

## Data Protection *Refer to the school Data Protection Policy*

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

- 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
- 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 Bursar or Head of Computing as soon as possible. *This also applies to cameras that may contain images of children*.**

## Communications - Staff and Pupils

The following table shows how the school currently considers the benefit of using these technologies for education balances against their risks / disadvantages:

| | Staff & other adults | | | | Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allows | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | ✓ | | | | | | ✓ | |
| Use of mobile phones in lessons | | | ✓ | | | | | ✓ |
| Use of mobile phones in social time | | ✓ | | | | | ✓ | |
| Taking photos on school mobile phones or other school camera devices (excludes EYFS) | ✓ | | | | | | ✓ | |
| Taking photos / videos on personal devices | | | | ✓ | | | | ✓ |
| Use of other mobile devices eg tablets, gaming devices | | ✓ | | | | | ✓ | |
| Use of personal e-mail addresses in school, or on school network | | ✓ | | | | | ✓ | |
| Use of school e-mail for personal e-mails | | ✓ | | | | | ✓ | |
| Use of messaging apps | | ✓ | | | | | ✓ | |
| Use of social networking sites | | | ✓ | | | | ✓ | |
| Use of blogs | ✓ | | | | | | ✓ | |

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

- The official school e-mail service may be regarded as safe and secure. It is strongly recommended that staff and pupils should use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that e-mail communications may be monitored
- Users must immediately report, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and pupils or parents/guardians (e-mail, chat) must be professional in tone and content. These communications should only take place on official school systems.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

- All Prep school pupils from Year 5-8 will be issued with a school email address which can be used to communicate with staff. This is not currently accessible from home and pupils will learn about using email responsibly as part of their ongoing e-safety education.

## Social Media - Protecting Professional Identity

We all have a duty of care to provide a safe learning environment for pupils and staff, and could be held responsible, indirectly, for acts by 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 Sunninghill liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to Sunninghill
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. They should be set to 'private'.

Sunninghill official social media accounts are updated and monitored by the Head of Marketing/Admissions – Amanda Jones.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

The school's use of social media for professional purposes is checked periodically by the bursar to ensure compliance with school policies.

## Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. Usage is restricted as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | pornography | | | | X | |
| | promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | | |
| | any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy | | | | | X | |
| Infringing copyright | | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | | X | |
| On-line gaming (educational) | | | ✓ | | | |
| On-line gaming (non educational) | | | | | ✓ | |

| | | | | | |
|---|---|---|---|---|---|
| On-line gambling | | | | ✓ | |
| On-line shopping / commerce | | ✓ | | | |
| File sharing | ✓ | | | | |
| Use of social media | | ✓ | | | |
| Use of messaging apps | | ✓ | | | |
| Use of video broadcasting eg Youtube | ✓ | | | | |

## Responding to incidents of misuse

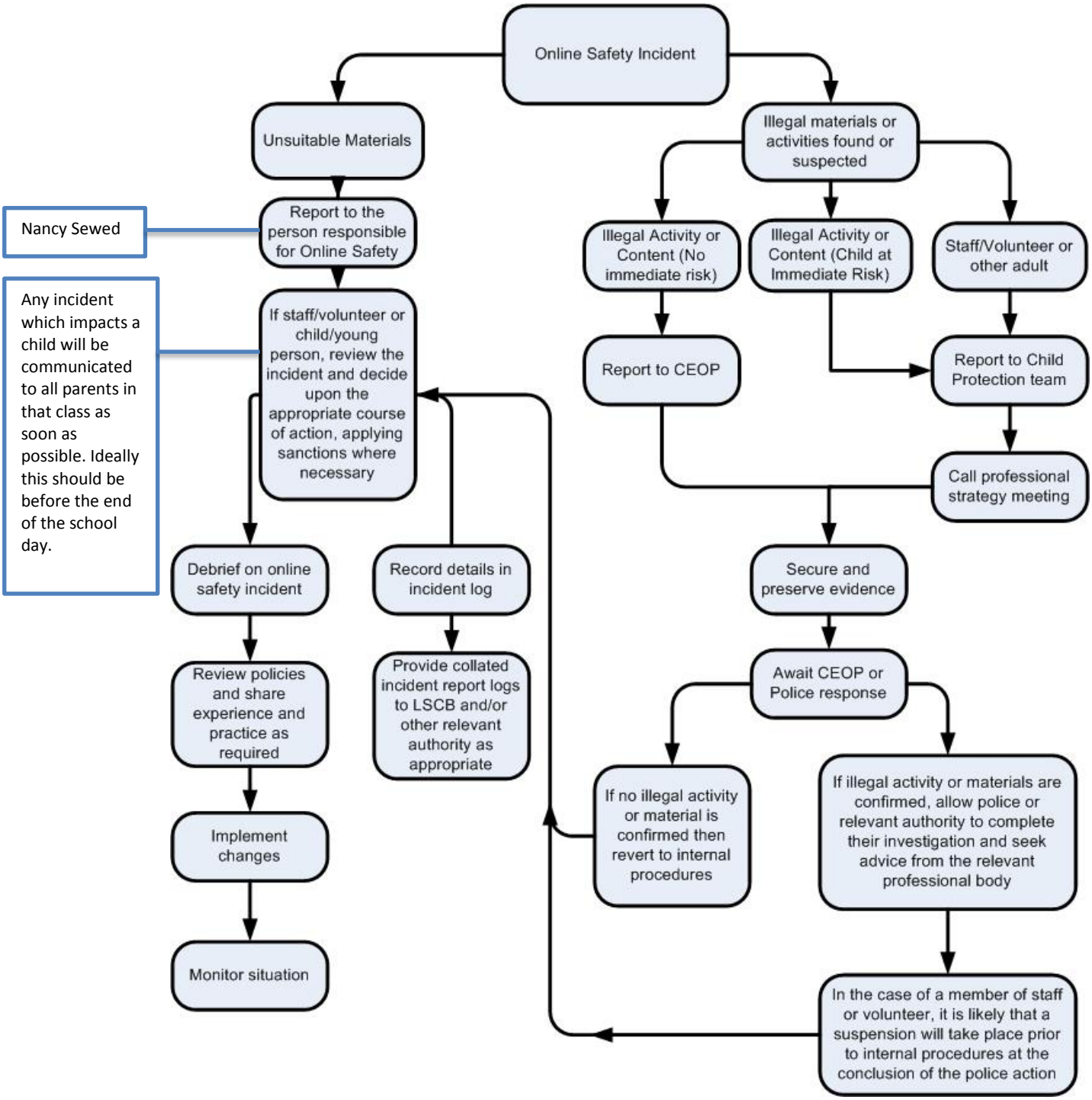
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

## 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 for responding to online safety incidents and report immediately to the police.
http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/creating-an-esafety-policy

## Unsuitable Images

Follow the left hand side of the flowchart.



### Other Incidents – procedure staff are to follow

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (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
- **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.

## 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 will be dealt with through normal behaviour / disciplinary procedures as follows:

## Pupils — Actions / Sanctions

| Incidents: | Refer to class teacher / tutor | Refer to DSL or Head of Computing | Refer to Head | 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 sanction eg detention |
|---|---|---|---|---|---|---|---|---|---|
| **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 use of mobile phone / digital camera / other mobile device | ✓ | ✓ | | | | | | | |
| Unauthorised 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 student's / 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 / academy'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 | ✓ | ✓ | | | | | | ✓ | |

## Staff Actions / Sanctions

| Incidents: | Refer to Head of Computing | Refer to Head | Refer to bursar | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **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 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 | | ✓ | | | ✓ | | | ✓ |

## Useful Resources:

**Safe Schools Team** - run in school e-safety sessions https://dcdhub.org/school-brochure/
Email: ssct@dorset.pnn.police.uk
Tel: 01202 222844

**UK Safer Internet Centre** https://www.saferinternet.org.uk/
SWGfL (South West Grid for Learning) - https://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - https://www.saferinternet.org.uk/professionals-online-safety-helpline
Internet Watch Foundation - https://www.iwf.org.uk/

**CEOP (Child Exploitation and Online Protection Command)**
**https://www.ceop.police.uk/safety-centre/**
ThinkUKnow - https://www.thinkuknow.co.uk/

**Others**
INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

**Online Safety Audit Tool**
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying
Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

**Social Networking Resources**
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

**Curriculum**
SWGfL Digital Literacy & Citizenship curriculum
Insafe - Education Resources

**Mobile Devices / BYOD**
Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

**Professional Standards / Staff Training**

DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

**Infrastructure / Technical Support**

Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

## Working with parents and carers

Dorset Police SSCT (Safe School and Communities Team) publish useful e-safety newsletters available here: Stop Think Dorset parents e-safety newsletters.
Parenting in the Digital Age (or PitDA for short): Parenting in the Digital Age Website
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

## Data Protection

Information Commissioners Office:
Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL - Guidance for Schools on Cloud Hosted Services
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

## Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015