

ST. CHAD'S C.E.(C) PRIMARY SCHOOL

E SAFETY Policy

"Building Together, with Jesus, for a better future"

Background

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

The Education and Inspections Act 2006 empowers Headteachers 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.

The school 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 the school.

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 Safeguarding Sub Committee receiving regular information about online safety incidents and monitoring reports. 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 Co-ordinator
- attendance at E Safety Group meetings- Safeguarding sub committee
- regular monitoring of E safety incident logs
- regular monitoring of filtering / change control logs- controlled by CCSC
- reporting to relevant Governors Committee meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E Safety Co-ordinator - the Headteacher at St Chad's.
- The Headteacher 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 online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the E Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders 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. Securus software is regularly monitored by CCSC.
- The Senior Leadership Team will receive regular monitoring reports from the E Safety Co-ordinator.

E Safety Coordinator:

The role of this coordinator is to:

- leads the E Safety agenda items on the Governors Safeguarding subcommittee
- 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
- liaises with school technical staff at CCSC
- receives reports of E safety incidents and creates a log of incidents to inform future E safety developments,
- meets regularly with E Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The school's network is managed by Chesterton Community Sports College CCSC. They are 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 online safety technical requirements and any Local Authority 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;**
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; Senior Leaders; E Safety Coordinator for investigation / action / sanction;
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current school E Safety Policy and practices;**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);**
- **they report any suspected misuse or problem to the Headteacher; Senior Leader ; Online Safety Coordinator for investigation / action / sanction;**
- **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 activities
- pupils understand and follow the E Safety Policy and acceptable use policies;
- 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 and that processes are in place for dealing with any unsuitable material that is found in internet searches.**

Designated Safeguarding Person

Should be trained in E Safety issues and be aware of the potential for serious child protection / safeguarding 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
- cyber-bullying

Governors Safeguarding Subcommittee

The Safeguarding sub committee is a group with responsibility for issues regarding E safety and the monitoring the E safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Safeguarding sub committee will assist the E Safety Coordinator with:

- the production / review / monitoring of the school E Safety Policy / documents.
- the production / review / monitoring of the school filtering policy) and requests for filtering changes.
- mapping and reviewing the E safety curricular provision - ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders - including parents / carers and the students / pupils about the E safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement**
- 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 online 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 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
- their children's personal devices in the school

Community Users

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

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. The education of pupils 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 Computing / PHSE and Character / other lessons and should be regularly revisited**
- **Key E safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **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**
- **Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.** *Nb. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.*

- Pupils should 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 and that 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 (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

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.

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Education – The Wider Community

The school will provide opportunities for 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
- E safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide E safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their E Safety provision.

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 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.**
- **All new staff should receive E safety training as part of their induction programme, ensuring that they fully understand the school E Safety Policy and Acceptable Use Agreements.**
- It is expected that some staff will identify E safety as a training need within the performance management process.
- The E Safety Coordinator will receive regular updates through attendance at external training events 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 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 subcommittee.. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

Unsuitable / inappropriate 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. 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. 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 / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

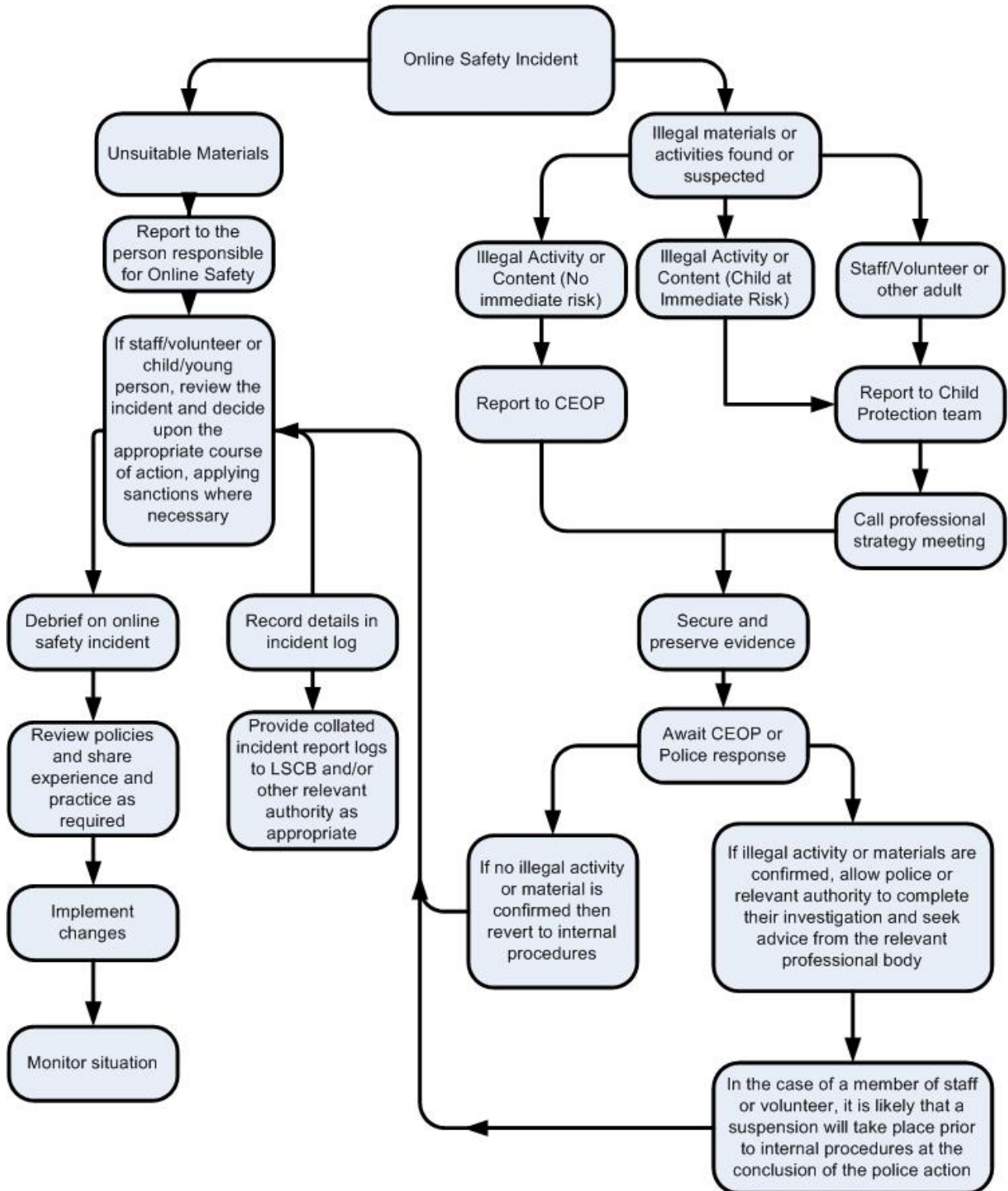
| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|--|--|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| Users shall not visit Internet sites, 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 | | | | X | |
| | 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) | | X | | | | |
| On-line gaming (non-educational) | | | | X | | |
| On-line gambling | | | | X | | |
| On-line shopping / commerce | | X | X | | | |
| File sharing | | | X | | | |
| Use of social media | | | | X | | |

| | | | | | |
|--|---|--|--|---|--|
| Use of messaging apps | | | | x | |
| Use of video broadcasting e.g. Youtube (for educational purposes only) | x | | | | |

Responding to incidents of misuse

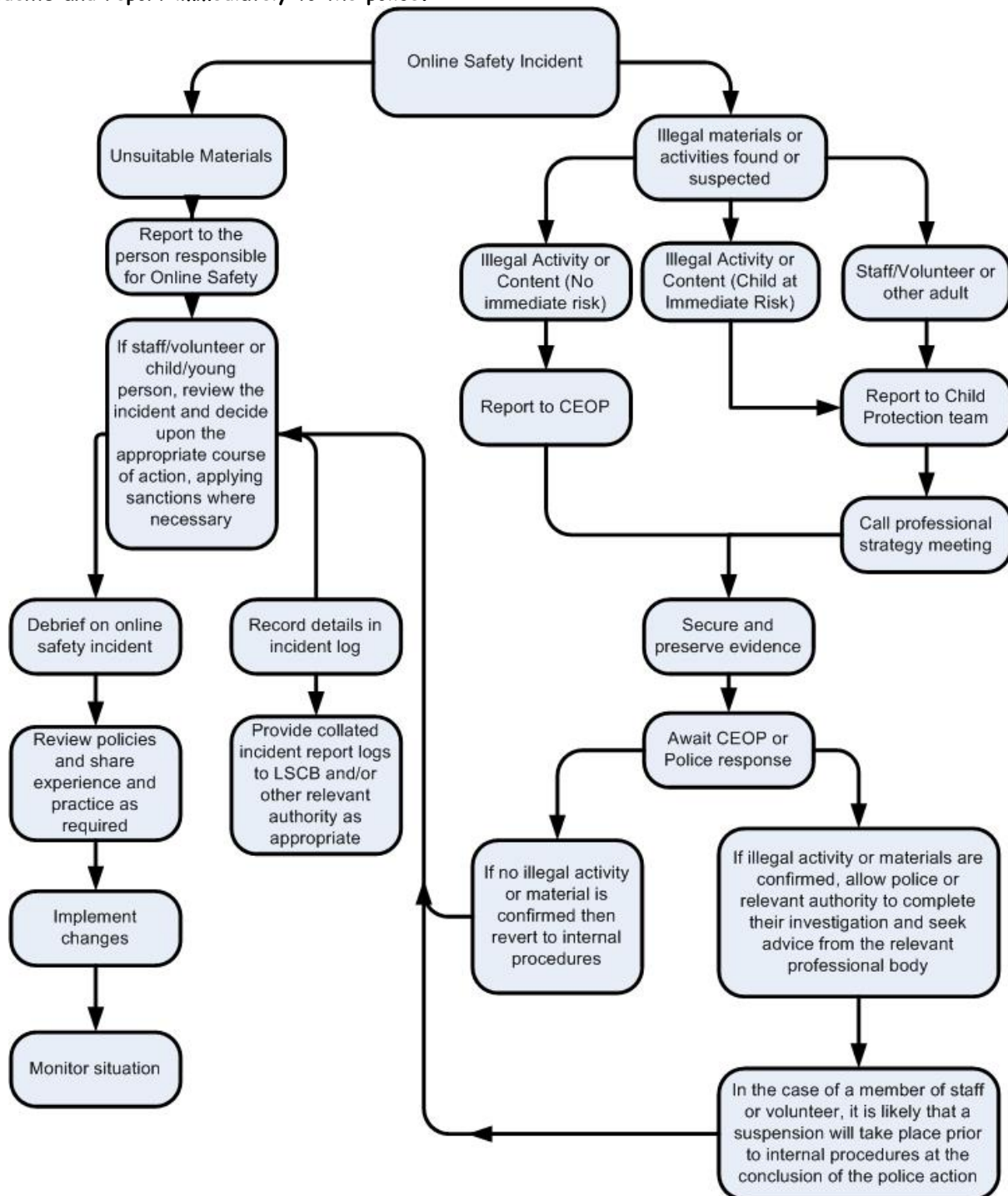
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

Responding to incidents of misuse - flow chart



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 for responding to E 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:
 - Internal response or discipline procedures
 - Involvement by Local Authority / Academy Group 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 safeguarding 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 Incidents | Actions / Sanctions | | | | | | | | |
|--|------------------------|-------------------------|----------------------|-----------------|---|-------------------------|---|---------|---|
| | Refer to class teacher | Refer to Senior Leaders | 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 sanction eg detention / exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | X | x | x | x | x | x |
| Unauthorised use of non-educational sites during lessons | x | x | x | | | X | | x | |
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | x | x | x | | | X | | X | |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | x | x | x | | | x | x | X | |
| Unauthorised downloading or uploading of files | x | x | x | | | | | X | |
| Allowing others to access school / academy network by sharing username and passwords | x | x | x | | | x | X | X | |
| Attempting to access or accessing the school / academy network, using another student's / pupil's account | x | x | x | | | x | X | x | X |
| Attempting to access or accessing the school / academy network, using the account of a member of staff | x | x | x | | | x | x | X | X |
| Corrupting or destroying the data of other users | x | x | x | | | x | x | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | x | x | x | | | x | x | | X |
| Continued infringements of the above, following previous warnings or sanctions | | | x | | | x | X | | x |
| Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school | | | x | | | x | x | | X |
| Using proxy sites or other means to subvert the school's / academy's filtering system | x | x | x | | | x | x | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | x | x | | | x | x | X | |
| Deliberately accessing or trying to access offensive or pornographic material | x | x | x | x | | x | x | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | x | x | x | | | x | x | | X |

| | Actions / Sanctions | | | | | | | |
|---|------------------------|----------------------|--------------------------------|-----------------|---|---------|------------|---------------------|
| | Refer to Senior Leader | Refer to Headteacher | Refer to Local Authority / LAD | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
| Staff Incidents | | | | | | | | |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | X | x | | X | x |
| Inappropriate personal use of the internet / social media / personal email | | x | | | x | X | | |
| Unauthorised downloading or uploading of files | x | x | | | x | X | | |
| 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 | x | x | | | | X | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | x | x | x | | x | X | | |
| Deliberate actions to breach data protection or network security rules | x | x | x | | x | | x | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | x | x | x | | x | | x | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | x | x | x | | x | | x | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | x | x | x | | x | | X | X |
| Actions which could compromise the staff member's professional standing | x | x | x | | | X | | |
| Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy | x | x | x | | | | | X |
| Using proxy sites or other means to subvert the school's / academy's filtering system | x | x | x | | | X | X | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | x | x | | | X | | |
| Deliberately accessing or trying to access offensive or pornographic material | x | x | x | x | x | | x | x |
| Breaching copyright or licensing regulations | x | x | x | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | x | x | x | | | | x | x |

E Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the [school/ academy] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (n.b. in small schools one member of staff may hold more than one of these posts):

[add/delete where appropriate]

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- *Student / pupil representation - for advice and feedback. Student / pupil voice is essential in the make-up of the online safety group, but students / pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Co-ordinator (or other relevant person) with the following [add/delete where relevant]:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through[add/delete as relevant]:
- Staff meetings
- Student / pupil forums (for advice and feedback)

- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference have been agreed

Signed by (SLT):

Date:

Date for review:

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication.

Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission.

This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre - <http://saferinternet.org.uk/>

South West Grid for Learning - <http://swgfl.org.uk/>

Childnet - <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

CEOP

CEOP - <http://ceop.police.uk/>

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/>

Tools for Schools

Online Safety BOOST - <https://boost.swgfl.org.uk/>

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/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -

<http://www.scotland.gov.uk/Publications/2013/03/7388>

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

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](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Teach Today - www.teachtoday.eu/

Insafe - [Education Resources](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information - Resources for Schools - ICO](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[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](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

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

[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](#)

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](#)

Glossary of Terms

| | |
|-------------------|--|
| AUP / AUA | Acceptable Use Policy / Agreement - see templates earlier in this document |
| CEOP | Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| CPD | Continuous Professional Development |
| FOSI | Family Online Safety Institute |
| ES | Education Scotland |
| HWB | Health and Wellbeing |
| ICO | Information Commissioners Office |
| ICT | Information and Communications Technology |
| ICTMark | Quality standard for schools provided by NAACE |
| INSET | In Service Education and Training |
| IP address | The label that identifies each computer to other computers using the IP (internet protocol) |
| ISP | Internet Service Provider |
| ISPA | Internet Service Providers' Association |
| IWF | Internet Watch Foundation |
| LA | Local Authority |
| LAN | Local Area Network |
| MIS | Management Information System |
| NEN | National Education Network - works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain. |
| Ofcom | Office of Communications (Independent communications sector regulator) |
| SWGfL | South West Grid for Learning Trust - the Regional Broadband Consortium of SW Local Authorities - is the provider of broadband and other services for schools and other organisations in the SW |
| TUK | Think U Know - educational online safety programmes for schools, young people and parents. |
| VLE | Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting, |
| WAP | Wireless Application Protocol |
| UKSIC | UK Safer Internet Centre - EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation. |

Approved: Summer 19
Review: Summer 20