ONLINE SAFETY AND ICT ACCEPTABLE USE POLICY

Version: 1.0
Approved: 4 December 2019
Next review: December 2022
Co-ordinator: Pat Sykes

Rationale

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and use of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's 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 online safety behaviour that take place out of school.

Purpose

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

Schedule for development/monitoring/review

The implementation of this Online Safety and ICT Acceptable Use Policy will be monitored by the:	*Online Safety Co-ordinator and Safeguarding Lead*
Monitoring will take place:	*Annually*
The designated Child Protection/Online Safety Governor will receive a report on the implementation of the Online Safety and ICT Acceptable Use Policy generated by the monitoring group:	*Annually*
School Council will review the Online Safety and ICT Acceptable Use Policy and will evaluate the effectiveness of procedures at their level:	*School Council meetings termly*
Should serious online safety incidents take place, these will be referred to the DSL in line with the school's Child Protection procedures:	*DSL Mrs Lucy Wanstall lucy.wanstall@sandwich-tech.kent.sch.uk*

The school will monitor the impact of the policy using:

- logs of reported incidents;
- monitoring logs of internet activity (including sites visited);
- internal monitoring data for network activity;
- surveys/questionnaires of:
  - students;
  - parents/carers;
  - staff.

Implementation

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

The Governors' Learning and Development Team is responsible for ensuring that an Online Safety and ICT Acceptable Use Policy is in place. The Governing Body has appointed a designated Child Protection/Online Safety Governor and, as part of his/her remit, he/she will receive monitoring reports and annual information about online safety incidents. The role of the Child Protection/Online Safety Governor will include:

- monitoring of online safety incident logs;
- monitoring of filtering/change control logs;
- reporting to relevant Governor meetings.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and the Online Safety Co-ordinator 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. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/HR/other relevant body disciplinary procedures.)
- The Headteacher and the Online Safety Co-ordinator are responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues as relevant.
- The Headteacher and the Online Safety Co-ordinator will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online Safety Co-ordinator

The Online Safety Co-ordinator:

- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- liaises with school technical staff;
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- provides monitoring reports and annual information about online safety incidents to the designated Child Protection/Online Safety Governor;
- provides training and advice for staff;
- provides training and advice for parents;
- provides training and advice for students;
- attends CEOP training;
- maps and reviews the online safety curricular provision – ensuring relevance, breadth and progression;
- reports to the Headteacher/DSL/Safeguarding Lead.

Network Manager/Technical Staff

The Network Manager/Technical Staff 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/other relevant body Online Safety Policy/guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;

- 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of the network/internet/Edulink/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Co-ordinator for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy;
- they report any suspected misuse or problem to the Online Safety Co-ordinator for investigation/action/ sanction;
- all digital communications with students/parents/carers are on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- students understand and follow the online safety and acceptable use policies;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras, etc, in lessons and other school activities (where permission is given) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned students are 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.

Child Protection/Safeguarding Designated Persons

Will receive regular training about online 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 incidences of grooming;
- social media.

Students:

- are responsible for using the school digital technology systems in accordance with the provisions of this policy;
- should 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 Online Safety and ICT Acceptable Use Policy covers their actions out of school, if related to their membership of the school;
- are required to read and observe the following protocol –
    - I know that school computers and internet access have been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed then I will ask a member of staff.
    - I know that school computers and internet access may be monitored.
    - I will keep my password safe and private as my privacy, school work and safety must be protected.
    - I will write emails and messages carefully and politely as I know that they could be forwarded or seen by someone I did not intend.

- I know that people I meet online may not be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult and will always arrange to meet in a public place with an adult present.
- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment.
- I will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
- I understand that I must not download or share inappropriate pictures, videos or other material online.
- I will protect my personal information online at all times.
- I will only upload appropriate pictures or videos of others online if I have permission.
- I will only use my personal device/mobile phone in school if I have permission from a member of staff.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I will always check that any information I use online is reliable and accurate.
- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences.
- I will only change the settings on the computer if a teacher/technician has given me permission to do so.
- I know that use of the school's ICT system for personal financial gain, gambling, political purposes or advertising is not allowed.
- I understand that the school's internet filter is there to protect me and I will not try to bypass it.
- I know that, if the school suspects that I am behaving inappropriately with technology, enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I know that, if I do not follow this policy, sanctions may be imposed.
- If I am aware of anyone trying to misuse technology then I will report it to a member of staff.
- I will speak to an adult whom I trust if something happens that makes me feel worried, scared or uncomfortable.

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/Edulink 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/Edulink;
- their children's personal devices in the school.

Parents are expected to read, sign and endorse provisions surrounding e-safety that are defined within the Home-School Agreement.

Community Users

Community users who access school systems/website/Edulink as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement (AUA) before being provided with access to school systems.

Bring your own device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing in their own technologies in order to provide a greater freedom of choice and usability. The following systems are in place to ensure the online safety of all users:

- the school has a set of clear policies and procedures which ensure all stakeholders are clear about the expectations and responsibilities for all users;
- all online safety personnel have clear roles and responsibilities to ensure the safety of all stakeholders;
- mandatory training is undertaken for all staff;
- students receive training and guidance on the use of personal devices.

Use of digital and video images

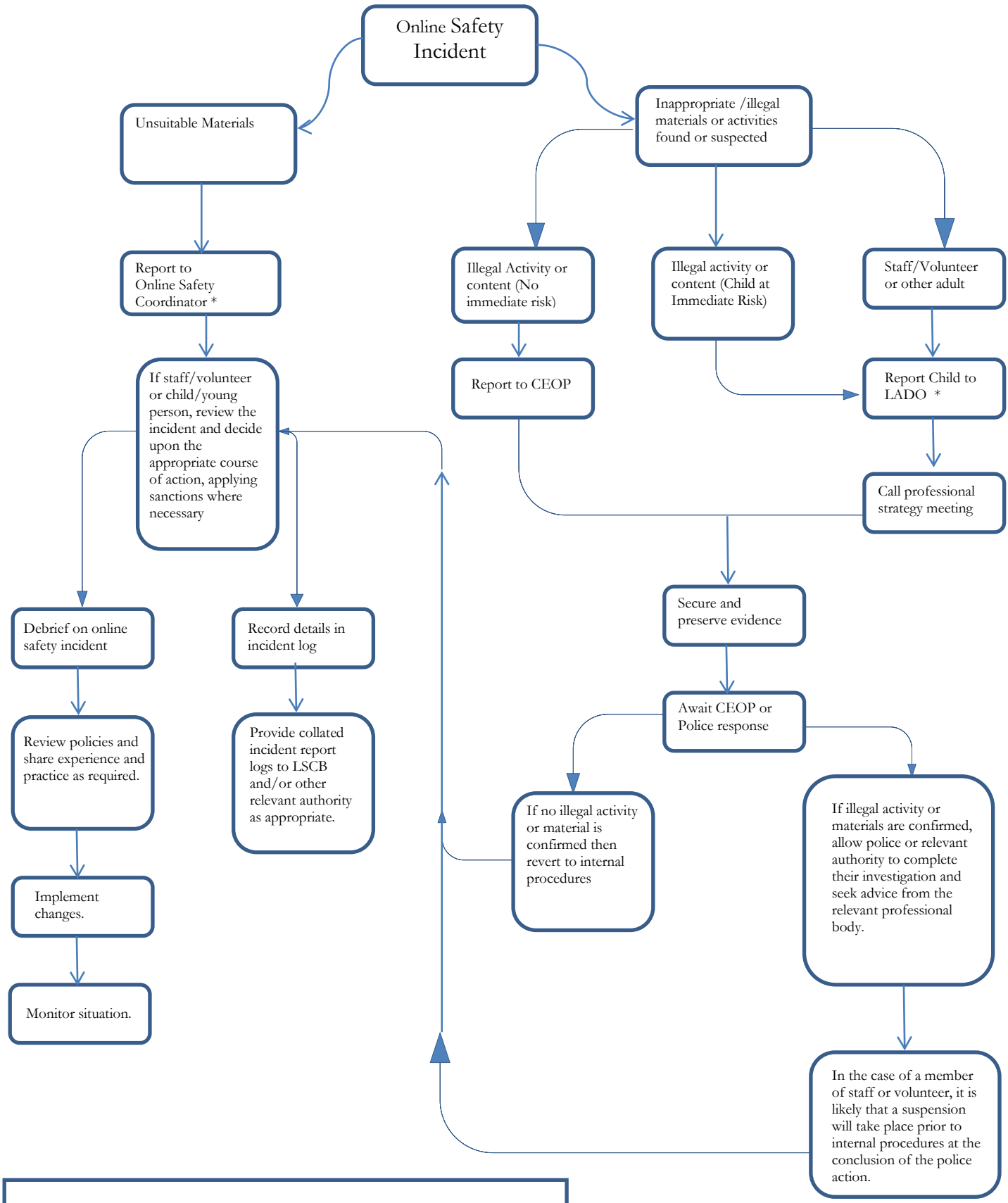
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- 'Keeping Children Safe in Education 2019' highlights the need for all members of staff to be aware that abuse can be perpetrated by children themselves, including sexting, and there is a need for all members of staff to handle "sexting" incidents as carefully as possible and offer support to all parties involved whilst abiding by the law and not compromising police investigations.
- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the student and parents or carers.

Links to other policies/documents

- Anti-bullying Policy
- Child Protection and Safeguarding Policy
- Home-School Agreement
- Student Behaviour Management Policy

Responding to incidents of misuse – flow chart



* liz.williamson@sandwich-tech.kent.sch.uk

*LADO – Angela Chapman 01233 898696 or 03000 411111

Reporting Log				
Student & College	Time/Date	Action Taken		Incident reported by
		What?	By Whom?	