THE DAWNAY SCHOOL

ONLINE SAFETY POLICY

Reviewed by:	**Paul Johnson, Andrew Rourke, Annette Di Giovanna**
Approved by Governors:	**Autumn 2018**
Review Date:	**Summer 2019**
Responsibility:	**FGB**
Status:	**recommended**

Based on Surrey County Council model policy and revised in reference to "Keeping children safe in Education" Update 2018

Document Status

The Online-Safety Policy relates to other policies, particularly those for ICT, behaviour, bullying and safeguarding (for "sexting" see the Child Protection and Safeguarding Policy). It was revised in autumn 2018 to ensure the content reflects current on-line safety advice.

The school Online-Safety Co-ordinator is Paul Johnson, who is the Computing subject leader and has been CEOP trained. The ultimate responsibility for online safety falls within the remit of the DSL, as online safety is a safeguarding issue. The DSL is Josephine Snell. Josephine Snell will be having the relevant CEOP training as soon as possible this year. The Computing subject leader and the DSL work in partnership as these roles overlap. The DSL delegates some of the activities regarding online safety to the Online-Safety Co-ordinator, for example areas connected with curriculum knowledge and specific technical knowledge and skills; however, as only safety is clearly identified as a safeguarding priority, the ultimate responsibility lies with the DSL.

Our Online-Safety Policy has been written by the Online-Safety Co-ordinator and the DSL, building on best practice and government guidance. It has been agreed by the Headteacher and approved by the governors.

The Online-Safety Policy and its implementation will be reviewed annually.

Teaching and learning

The use of technology has become a significant component of many safe -guarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

Our approach to online safety serves to protect and educate the whole school or in their use of technology and has mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues in Online Safety is considerable, but can be categorised into three areas of risk:

Content
Being exposed to illegal, inappropriate or harmful material (for example pornography, fake news, racist or radical and extremist views)

Contact
Being subjected to harmful online interaction with other users (for example commercial advertising as well as adults posing as children or young adults)

Conduct

Personal online behaviour that increases the likelihood of, or causes harm (for example making, sending and receiving explicit images, or online bullying)

At The Dawnay, pupils will be taught how to keep themselves (and others) safe online. They will be educated in the effective use of the internet in research, including the skills of knowledge location, validation, retrieval and evaluation. They will also be shown how to publish and present information appropriately to a wider audience and how to evaluate internet content.

Introducing the Online-Safety policy to pupils

Appropriate elements of the Online-Safety Policy will be shared with pupils and they will be taught how to report or block unpleasant Internet content using Hector Protector. Online-Safety rules will be posted in all networked rooms. Pupils will be informed that internet use in school will be monitored. Curriculum opportunities to gain awareness of Online-Safety issues, and how best to deal with them, are provided in each academic year.

Pupils will also be educated on the dangers of on-line chat (including through gaming and social media), how to spot the signs of cyber-bullying and what to do to prevent and/or resolve such issues.

The majority of this education comes from the "Be Internet Legends" scheme of work devised by ParentZone and Google, though other materials may be added to this as part of additional support (for example new activities for the annual Safer Internet Day) or in response to a new concern.

Managing Internet Access

The school's internet access is provided by Surrey County through 'RM" and filtration (and reporting) is through "RM safety net plus". For a more technical breakdown of the filtration, please see their website (http://www.rm.com/products/online-safety-tools/rm-safetynet).

It is important, however, to recognise that no filtering systems can be 100% effective but we help protect our children with good teaching, learning practice and effective supervision. Also, it is recognised that "overblocking" can place unreasonable restrictions on what children can be taught.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online-Safety Co-ordinator, DSL and Head Teacher.

School ICT systems security and virus protection software will be reviewed regularly. Security strategies will be discussed with the Local Authority.

Children are not permitted access to their mobile phones on entering the school site and must surrender their device to the school office where it will be held until the end of the school day.

All staff are able to log in to the school's network remotely to reduce the need for sensitive material to be stored on personal computers or be carried on memory sticks.

E-mail

Pupils and staff may only use approved e-mail accounts for class use. The details (including passwords) for these accounts are held by the Computing subject leader and the Bursar. Staff and pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils will be instructed not to reveal personal details of themselves or others in e-mail communication, nor arrange to meet anyone without specific permission.

Staff to pupil email communication must only take place via a school email address and will be monitored. Staff are referred to Section 13 of the Staff Behaviour Policy (Code of Conduct), which details responsible email use for members of staff.

Incoming e-mail should be treated with care and attachments not opened unless the author is known.

Published content and the school web site

The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published (with the exception of staff names).

The Deputy Head teacher and Bursar will take overall editorial responsibility and ensure that content meets statutory requirements, is accurate and appropriate.

Publishing pupils' images and work

Parental permission will be sought to use photographs for both internal (e.g on display work or as part of a medical notice board) and external use (i.e on the website or the school's APP). Note that those photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will seek to use group photographs rather than full-face photos of individual children. However, for marketing or celebratory purposes photographs of children may be used but this will always be with the agreement of parents.

Pupils' names will be avoided on the website particularly in association with photographs, however, newsletters are published on the website and often contain photographs and names so full names will never be used.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories (e.g. mobile apps, Twitter feeds and local news websites)

Social networking

The school blocks access to social networking sites, and strives to educate pupils in their safe use e.g. use of passwords, never to give out personal details of any kind which may identify them or their location. They will be advised to use nicknames and avatars when using social networking sites.

Pupils and parents will be advised, in training provided by the Online-Safety Co-ordinator, that the use of social network spaces outside of school should be carefully monitored and will be made aware of the potential hazards that they may encounter.

Pupils must not place inappropriate personal information on network space provided on the school's shared network.

Staff are referred to Section 13 of the Staff Behaviour Policy (Code of Conduct), which details responsible social-media use for members of staff.

Authorising internet access

In Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

In Key Stage 2 access is less directed but **AN ADULT MUST BE PRESENT AT ALL TIMES.**

Parents will be asked to sign and return a consent form.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, **it is not possible to guarantee that unsuitable material will never appear on a school computer**. Neither the school nor SCC can accept liability for the material accessed, nor any consequences of internet access, providing all necessary measures are in place.

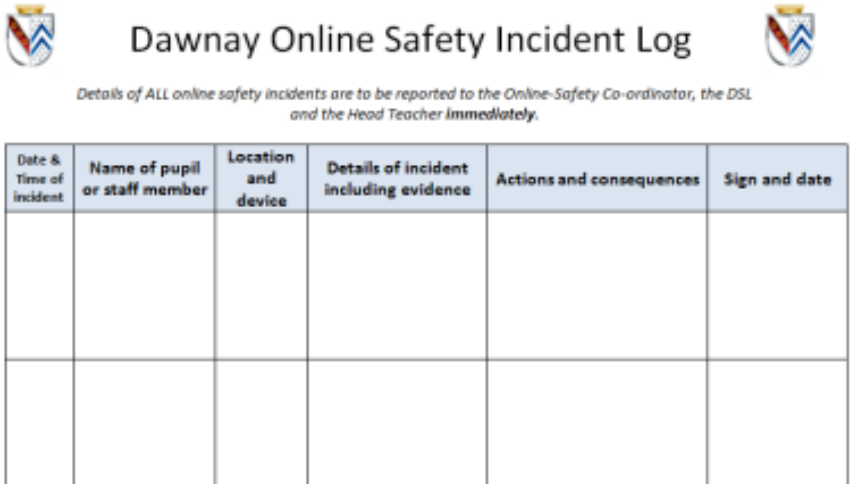
Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Online-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access) and virus notifications must be reported to the Online-Safety Coordinator.

Any online-safety issues which specifically relate to the Safeguarding of pupils (e.g. cyber-bullying, child sexual exploitation, radicalisation and sexual predation) must be reported immediately to the DSL or the Deputy DSL, and also to the Online Safety Co-ordinator.

Online-Safety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns. The below is a screen grab of the Dawnay Online Safety Incident Log.



Dawnay Online Safety Incident Log

Details of ALL online safety incidents are to be reported to the Online-Safety Co-ordinator, the DSL and the Head Teacher ***immediately****.*

Date & Time of incident	Name of pupil or staff member	Location and device	Details of incident including evidence	Actions and consequences	Sign and date

The Log itself is kept in the DSL's locked cupboard in the DSL/SENCo's Office. Completed copies should be given to the DSL as soon as possible after completion. Completed copies should be in hard-copy form and should be signed and dated by the person(s) who observed the incident.

A soft-copy template of the Log is stored in: staff/ computing/online safety area of the school's shared network, and a hard-copy template can also be obtained from the DSL and Online-Safety Co-ordinator.

Handling Online-Safety complaints

Complaints or concerns regarding Online-Safety issues will be dealt with by the Phase Leaders and involve the Online-Safety Co-ordinator and (where appropriate) the Head teacher or Deputy Head teacher. Any complaint about staff misuse must be referred to the Head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure.

Community use of the internet

All use of the school internet connection by community and other organisations shall be in accordance with the school acceptable user agreement. Any before or after school hours groups who wish to use the school's Internet must ensure that their pupils and staff sign up to the Acceptable Use Agreement (unless they have already done so).

Mobile phone/device/camera usage

The use of mobile technology and its potential to impact upon child protection has increased dramatically over the last five years. Therefore we do not allow staff members to use their own devices (cameras, phones or other mobile technology) to record/capture images of children. The school's own devices must be used for recording images of children and these images must be kept within school unless permission is given.

Staff are referred to the Staff Code of Conduct which detail responsible mobile phone/device/camera use for members of staff.

Children are not given access to their own mobile devices when in school.

Staff and the Online-Safety Policy

All staff are given the school's Online-Safety Policy and the Acceptable Use Policy at induction, and their importance is explained. They will be made aware that internet traffic can be monitored and traced to the individual user and that discretion and professional conduct is essential. Finally they will be asked to sign the school's 'Acceptable user agreement' which précis all of the above. All staff are given a copy of the Staff Behaviour Policy (Code of Conduct) which, in Section 13, deals with Online Safety.

Enlisting Parents' and Carers' support

Parents' and Carers' attention will be drawn to the school's Online-Safety Policy in newsletters and on the school's website. Parents and Carers will be provided with additional information on Online-Safety from time to time. The school will ask all new Parents to sign the Parent/pupil agreement each year.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 AND following the school's guidance in the document "Data Security Poster for Staff 2018".

Relevant policies and agreements:

Acceptable use agreement (staff) and (home – pupil and parent)
Child Protection and Safeguarding Policy

Staff Behaviour Policy (Code of Conduct)
ALSO: “Data Security Poster for Staff 2018”.

Relevant websites
www.thinkuknow.co.uk
http://www.rm.com/products/online-safety-tools/rm-safetynet