Danson Primary School

E-Safety Policy / Acceptable Use Policy

Introduction and Overview:

The policy is provided to all staff and should be read in conjunction with the following policies:

- Safeguarding & Child Protection Policy
- Anti-Bullying Policy
- E-Safety Policy
- GDPR Policy
- Staff Code of Conduct Policy
- Whistle-blowing Policy

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Danson Primary school with respect to the use of ICT-based technologies.

- safeguard and protect the children and staff of Danson.

- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.

- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.

- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- minimise the risk of misplaced or malicious allegations made against adults who work with students.

'Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. 12. We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. 13. This advice brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach.'
(DfE-2019 Teaching online safety in school)

Online safety

135. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of

technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
136. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

137. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
(KCSIE 2022)

The main areas of risk for our school community can be summarised as follows:

Content:

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact:

- Grooming:
- cyber-bullying in all forms
- identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

Conduct:

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sharing nudes (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Who will write and review the policy?

- Our e–Safety Policy has been written by the school, building on the London Grid for Learning Guidance. It has been agreed by the Senior Leadership Team and approved by governors.
- Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement.
- When staff and pupils leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- The school will appoint an e-Safety leader who will oversee curriculum links and parent workshops.
- The e-Safety Policy and its implementation will be reviewed annually.

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates.

How can the Internet use enhance learning?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Remote education can enable children to access education remotely when they cannot attend school.

How will pupils learn how to evaluate Internet content?

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Virus protection will be updated regularly.

- Pupils will use age-appropriate tools to research internet content.

How will information systems security be maintained?

- Virus protection will be updated regularly.

- The security of the school information systems and users will be reviewed regularly.

- Unapproved software will not be allowed in pupils' work areas or attached to email.

- Files held on the school's network will be regularly checked.

- The ICT co-ordinator / network manager will review system capacity regularly.

- The use of user logins and passwords to access the school network will be enforced.

- The use of 2 factor authentication for those members of staff who have access to highly sensitive information will be expected.

How will e-mail be managed?

- Staff should not use personal email accounts during school hours or for professional purposes.

Staff should not use their school email accounts for non-school based (personal) activities or purposes.

- Whole-class or group email addresses will be used for communication outside of the school.

- Access in school to external personal e-mail accounts may be blocked.

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Emails may be quarantined due to them containing identifiable or sensitive information and will be released by the Network Manager when satisfied or approved by the Head Teacher.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT').
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The E- Safety Leader, Office Manager and SLT will take overall editorial responsibility and ensure that content is accurate and appropriate.

Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Pupils work can only be published with their permission or their parents/carers.

How will social networking, social media and personal publishing be managed?

- The schools will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

Students should be encouraged to invite known friends only and deny access to others.

- Students should be advised not to publish specific and detailed private thoughts.

How will filtering be managed?

- If staff or pupils discover unsuitable sites, the URL must be reported to the E- Safety Leader. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- The E- Safety Leader, Network Manager and SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- School has incorporated 'Securly' software as an additional measure that is overseen by SLT and DSL.

How will videoconferencing be managed?

- When recording an online/virtual meeting or lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of online/virtual meeting should be clear to all parties at the start of the meeting. Recorded material shall be stored securely.

The equipment and network

- All online/virtual meeting equipment in the classroom must be switched off when not in use and not set to auto answer.

- External IP addresses should not be made available to other sites.

- Online/virtual meeting contact information should not be put on the school Website, unless approved by the Head Teacher.

- The equipment must be secure and if necessary locked away when not in use.

- School online/virtual meeting equipment should not be taken off school premises without permission.

Users

- Parents and carers should agree for their children to take part in online/virtual meeting, probably in the annual return.

- Unique log on and password details for the educational online/virtual meeting services should only be issued to members of staff and kept secure.

Content

- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

- Online/virtual meeting should be supervised appropriately for the pupils' age.

- Establish dialogue with other conference participants before taking part in an online/virtual meeting. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time (as part of the School AUP).
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices by any member of the school community is forbidden and any breaches will be dealt with as part of the school discipline/behaviour policy.

- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team in the presence of a parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Danson's Network

- Do not store personal information or non-work related material on the school system.
- Consult IT Department before storing large video and photo files.
- Do not copy centrally available files to personal user areas as this duplicates files and wastes disk space.
- Use of removable of media (USB) is prohibited unless agreed with the Head Teacher.
- Any pictures or film more than 1 year old other than needed for evidence must be deleted from the system.
- Laptops/chromebooks must be placed in the hidden from view when being transported by car.

BYOD (Bring Your Own Device) and Personal Devices

Any personal equipment must be authorised by the Network Manager then Head Teacher before use on the School Network. All activities and Danson's Systems and Hardware will be monitored in according to the policy

- Staff are permitted to use Social Media on personal devices during non-contact time with children when in areas of the school away from the children

Care of Equipment

When in school, do not rearrange the way in which equipment is plugged (computers, power supplies, phones, network cabling) without first contacting the Network Manager.

Remote Access on a Personal Device

- Remote Access is provided to all staff via Google Apps for Education
- You are responsible for all activity
- Devices remotely accessing data must not be left attended
- Login information must not be written down or disclosed to anyone
- Any files downloaded to work on must be deleted once uploaded back to the system
- Documents must not be printed off on personal printers if they contain sensitive/personal information pertaining to staff, parents or children.
- Care should be taken when working in public places or transport that client information is not visible to other users.

Remote Access on a School Device

- Remote Access is provided to all staff via Google Apps for Education
- You are responsible for all activity
- Devices remotely accessing data must not be left attended
- Login information must not be written down or disclosed to anyone
- Take care of the device in protecting it from loss/theft/damage
- School owned devices should not be used by anyone else in your household

Use of Internet?

- The use of internet by employees is permitted and encouraged where such use encourages and supports the goals of the school.
- However when using the internet, employees they:
  - Comply with current legislation
  - Use in the internet in an acceptable way
  - Do not create unnecessary business risk by misuse of the internet

The following is deemed unaccepted use of the internet or behaviour of employees this list is non-exhaustive:

- Visiting internet sites that obscene, hatful, pornographic or other legal materiel
- Use of computer for fraud, software, film or music
- Use the internet to send hateful or harassing material to other users
- Downloading commercial software or any copyrighted materials belonging to 3rd parties unless covered under commercial agreement
- Hacking in to unauthorised areas
- Creating defamatory material
- Undertaking deliberate activities that waste employees or network resources

  - Do not look for, download, bookmark access material that may be regarded as obscene or pornography
  - Be aware of copyright law when using information found on other 3rd party websites

Confidentially

- If you are dealing with personal, sensitive and or confidential information then you must ensure that extra care is taken to protect the information by email then the following protocols should be used.
  - **If there any doubt as to the information being sent or the appropriate level of information required, please check with:**
    - **Business manager**
    - **Senior Leadership Team**
    - **Network Manager**
- Personal, sensitive and or confidential information should be contained in an attachment and appropriate case encrypted or password protected
- Any password or key must be sent separately
- Before sending the email verify the email address
- Do not refer to the sensitive information contained in the attachment in the email body.
- Emails can also be sent securely using Egress Web Access.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

- All staff must read and sign the Acceptable Use Policy before using any school ICT resource.

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

- Parents will be asked to sign and return a consent form for pupil access as part of the Home-School agreement.

How will risks be assessed?

- The school should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Bexley Local Authority can accept liability for the material accessed, or any consequences resulting from Internet use.

How will e-safety complaints be handled?

- Any complaint about staff misuse must be referred to the Head Teacher.

- Parents and pupils will need to work in partnership with staff to resolve issues.

- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.

- All e–Safety complaints and incidents will be recorded by the school on the 'E-Safety Incident Log' — including any actions taken.

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety.

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.

- There will be clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded on the E-Safety Incident Log

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

How will Learning Platforms and Learning Environments be managed?

- SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

- Pupils/staff will be advised on acceptable conduct and use when using the learning platform.

- Only members of the current pupil, parent/carers and staff community will have access to the LP.

- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.

How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.
- An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. This will be updated on an annual basis

- Pupil instruction in responsible and safe use should precede Internet access.

- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use. E-Safety lesson will be covered in each half term within the computing unit of work.

Classes have E-Safety Agreements and each class will be taught these and will sign to say that they will uphold the rules and behaviours within each of the Agreements.

- All users will be informed that network and Internet use will be monitored.

- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.

- Staff training in safe and responsible Internet use both professionally and personally will be provided.
-
- Accreditation of the school as a National Online Safety School will also provide staff with additional training and policy updates.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.

- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.
-
- Parents will be informed and encouraged to complete the National Online Safety courses and engage with their parental information posters to keep children safe whilst they are online at home.

Education at home: Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges and-other-providers and safeguarding-and-remote-education KCSIE 2020, p.104
This Policy will be reviewed if necessary with any legislative changes from the ICO (Information Commissioner's Office) and EU GDPR (General Data Protection Regulation) legislation.

All Employees, Volunteers and Contractors who have been granted the right to use Danson IT Systems sign this agreement understanding and confirming their expectance.

Title	Danson Primary School Staff Acceptable Use Policy
Version	9.0
Date	June 2023
Author	Head Teacher Computing/E-Safety Subject Leader Business Manager IT Network Manager
Approved by	Online Safety Governor June 2023
Approved by	Governing Body June 2023
Next review date	June 2025

Agreement Introduction

This document has been developed to ensure staff within Danson Primary School are aware of their professional responsibilities when using ICT equipment and systems. All staff will follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home. ICT equipment and associated technologies include all facilities and resources used to access the school ICT network and internet as well as standalone devices with digital storage. When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

General Usage:

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure.

- I will ensure my workstation is locked whenever I am going to leave it unattended

- I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the E-Safety leader, SLT and Network Manager

- All passwords I create will be in accordance with the school e-safety policy.

- I will ensure that I use a suitably complex password for access to the internet and ICT systems and that:
  -I will use a unique password for each system.
  -I will not share my passwords with any colleagues or pupils within school.
  -I will seek consent from the Computing leader/ Headteacher/DHT/Senior Leaders prior to the use of any new technologies (hardware, software, cloud-based services) within school.

- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the Computing leader/Headteacher/DHT/Senior Leaders.

- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.

- I will take a professional and proactive approach and will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site.

- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location).

- Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.

- I will secure any equipment taken off site for school trips.

- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/password protection deployed.

- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Computing Subject Leader/ Head Teacher/DHT/Senior Leaders (as appropriate)

- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site.

- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).

- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the IT Technician.

- I will return any school-owned ICT equipment or software to the relevant individual within school (ICT manager/technician) once it is no longer required, ensuring it is in a good working condition

- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

- I understand that if I do not follow all statements in this AUP and in other school's policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.

Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.

- I must not use social media tools to communicate with current or former pupils under the age of 18.

- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.

- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.

- Staff must not access social networking sites for personal use during school hours.

- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the E-Safety Leader or Head Teacher.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.

- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the E-Safety Policy/ Home School Agreement (or any other relevant policy).

- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff. (Computing leader or Headteacher).

- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.

- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.

- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and immediately deleted from the memory card.

- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Teaching and Learning

- I will support and promote the school E-Safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of Safety and know what to do in the event of misuse of technology by any member of the school community.

- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Email

- I will use my school email address for all correspondence with staff, parents, governors or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business or my school email for private business

- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.

- I will not synchronise any school email account with a personally-owned handheld device unless secured with password or suitable biometric protection (face unlock/fingerprint)

- I agree that by synching my mobile device to my work email, I/Danson Primary School have the ability to remotely wipe the device should it be lost or stolen

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders. Any emails that you're unsure of please email to IT Support

- Emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the Head Teacher, line manager or another suitable member of staff into the email.

- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders all emails we be purged after 120 days.

- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

- Danson reserves the right to monitor communications received my system users, employees and temporary users

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.

- Bluetooth communication will be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.

- I will not connect any mobile device to the schools wireless network at any time

- I will not connect any mobile device to the school network at any time

- I will not contact any parents or pupils on my personally-owned device unless prior permission has been sought from the Head Teacher (in the event of remote education or extenuating circumstances.)

- I will not use any personally-owned mobile device to take images, video or sound recordings.

Extract From Danson's Safeguarding and Child Protection Policy

Use of Technology

All staff in our school will use technology to support and promote the learning and welfare of the children. However certain safeguards should be remembered:

Mobile phones - Staff will NOT give any child their personal mobile phone number and will not contact the child on the child's mobile phone either by voicemail or by texting without the consent of the parent and in line with the school's policy in respect of use of mobiles. Staff should not use a mobile phone in the presence of school pupils and pupil areas of the school site unless it is an emergency. In relation to photographs, staff **must not** use their personal mobile phone, personal camera (still or moving images) or other devices to take, edit or store images of children from this school. Staff will have an absolute commitment to seek advice from a senior leader about any situation that may be capable of being understood as inappropriate.

Staff will ensure Bluetooth is disabled when on school premises on all personal mobiles and laptops.
Communication by email should only be through the school's email system and personal emails must not be shared with children. Staff should not communicate with pupils through private email accounts, social networking sites, even on educational matters, but must use official email and networking sites sanctioned by the school. Staff should be extremely careful in their personal use of social networking sites and must not discuss school business or any issues relating to pupils.
Use of Internet: Staff will NOT access or expose children or young people to unsuitable material on the internet. Staff will ensure that they follow e-safety standards about access to and use of the internet and be mindful of the Teacher Standards. The Head teacher will have the final decision on whether a member of staff has behaved in an inappropriate or unprofessional manner.

Examples of inappropriate conduct might include:

- Participating in chat rooms with pupils
- Use of a social media site such as Facebook or Twitter to communicate with pupils,
- Text-messaging
- The promotion of non-school activities such as outside clubs and organisations or
- Sending emails that are not directly related to the pupil/teacher relationship and specifically relating to school business

The school will make use of the powers to search pupils for items that the school deems as banned, inappropriate, a safeguarding risk or prevent the maintenance of good order and discipline, e.g. mobile phones.

E-Safety in *Danson Primary School*
Most young people experience the internet and mobile phones as a positive, productive and creative part of their activities and development of their identities. However, issues of E-Safety do arise as some students use the technologies negatively.

In Danson Primary School*,* we have a major responsibility to educate our pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, particularly social networking sites. It is also important to include parents as much as possible in this process given that children often have access to computers at home.

In Danson Primary School*,* we have a robust filter for the internet and a system for monitoring computer usage, which takes screen shots if any word from our 'trigger' list is typed. If a student is caught viewing inappropriate material on a computer or on their mobile phone via the School system during School hours, they will receive a serious sanction. However, out of School and particularly on mobile phones connected to the mobile networks, there is often no supervision, monitoring or filtering. See **A*ppendix 1*** for guidelines to support parents / guardians.

Cyber-bullying is unfortunately another area which is growing rapidly. It is different from more traditional forms of bullying. Some students have 24 hour access to the internet or a mobile phone and so it can be hard to escape. The audience for the bullying can be potentially huge and comments and pictures are likely to stay online forever.

The school is committed to working with Bexley LSCB to combat bullying.

As with all forms of bullying, the School will deal with this in accordance with the Behaviour Policies (particularly the Anti-bullying and Cyberbullying policies), even if the cyber-bullying is happening outside School hours.

If parents / guardians have any concerns that their child is being cyber-bullied, they should please print off any available evidence and report it to the School as soon as possible.

Agreement

I have read and understand all of the Danson School Staff, Governor and Volunteer Acceptable Use Policy relating to my use of technology within school. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Staff Name:

Signed:

Date:

APPENDIX 1-Online Safety-KCSIE 2023 (p35)

Online safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

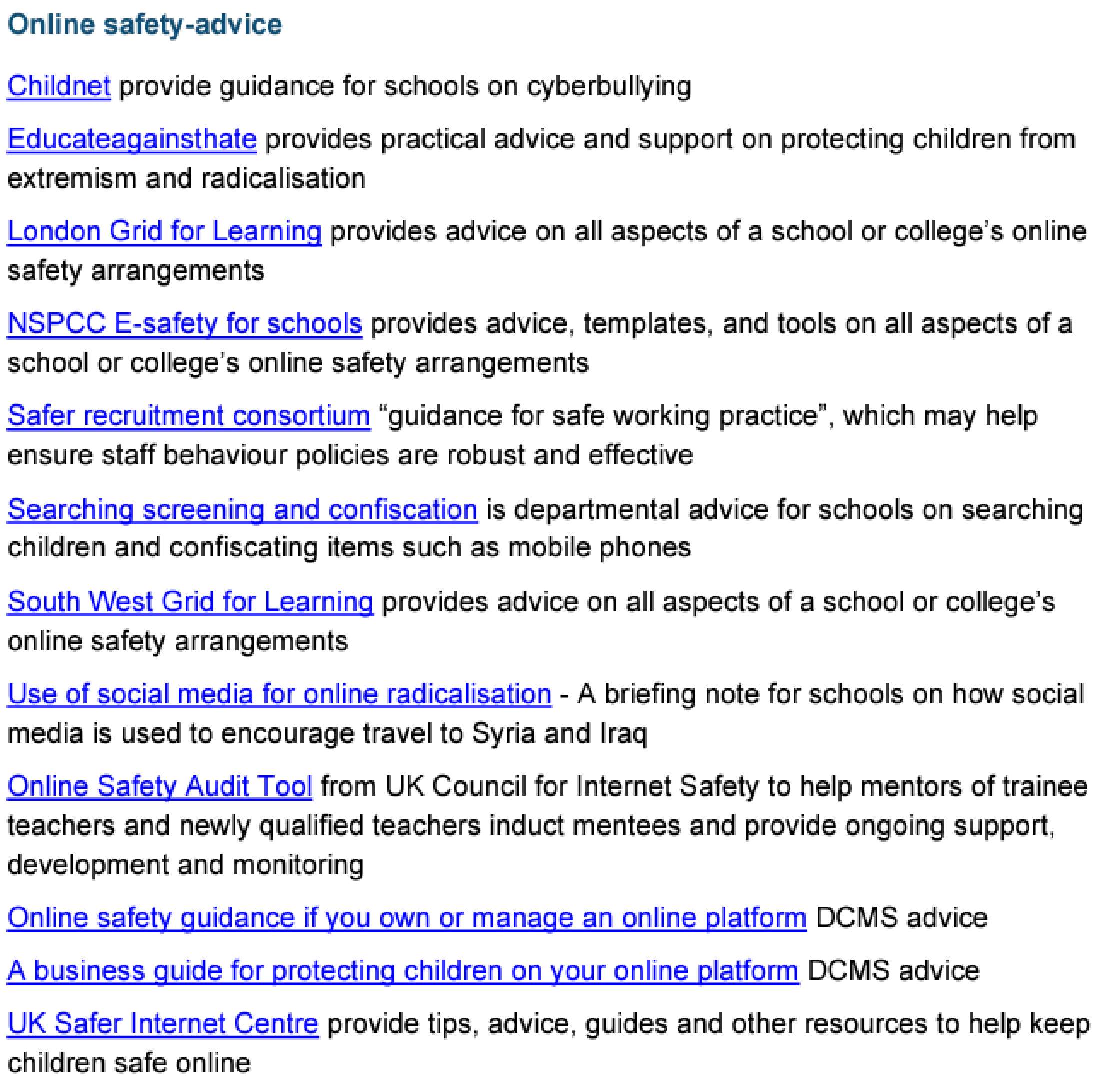
Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Remote education

Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and Providing remote education: guidance for schools - GOV.UK (www.gov.uk). The NSPCC also provide helpful advice - Undertaking remote teaching safely.
Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Filtering and monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.



Online safety-advice

Childnet provide guidance for schools on cyberbullying

Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college's online safety arrangements

Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

Online safety guidance if you own or manage an online platform DCMS advice

A business guide for protecting children on your online platform DCMS advice

UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Online safety- Remote education, virtual lessons and live streaming

Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students

Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely

London Grid for Learning guidance, including platform specific advice

National cyber security centre guidance on choosing, configuring and deploying video conferencing

Online safety- Parental support

Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online

Let’s Talk About It provides advice for parents and carers to keep children safe from online radicalisation

London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone’s behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

Parentzone provides help for parents and carers on how to keep their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children’s Commissioner's parental guide on talking to their children about online sexual harassment

#Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships

Reviewing online safety
Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCIS has published Online safety in schools and colleges: Questions for the governing board to help responsible bodies assure themselves that their online safety arraignments are effective.

Education at home

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges and-other-providers and safeguarding-and-remote-education

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on sharing nudes-in-schools-and colleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning 106 Support for children
- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sharing nudes, and cyberbullying

- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let’s Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone’s behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

APPENDIX 2

E-SAFETY GUIDELINES FOR PARENTS / GUARDIANS

Consider some of the points below to ensure that your child is using the fantastic new technologies available to them as safely as possible.

Please consider employing the strict "safe search" setting on Google. For more information on this and further guides you could look at www.candp-s.com/familysafety - a website full of useful material and advice on Online Safety.

2. Look into setting Parental Controls on a Windows Vista, Windows 7 or Mac computer to restrict specific web sites and also the time when the computer can be used.

3. Mobile phones offer children an amazing amount of opportunity in what they look at and what they can text, including picture messaging. If your child has a smart phone, then please consider setting safe searches on Google and YouTube on these as well.

4. Please take time to talk to your child about their use of the internet. It will be impossible and perhaps not even desirable to ban everything; indeed they are often much more able than us at using the computer! Education and dialogue are the only realistic ways to protect young people.

5. Please encourage a balanced use of the computer and mobile phones- for example, setting expectations that computers are off at 10pm and phones aren't used at mealtimes or ½ hour before bedtime (and not once in bed!).

***How a parent/carer can ensure that their child's online experience is safe.**
Learn - Find out more about online threats
Talk - Discuss what your child should, and should not, do online and print off a copy of the Safe Internet Use Agreement **-** sign it and put it on the wall.
Have fun - Enjoy some of the recommended sites by going online together (let your child show you how).
Take action - Make searching on the internet safer by blocking pornography on Google and YouTube and get a healthy balance by setting time restrictions on your child's computer.
Care - Make each child's computer use more comfortable – avoid posture problems by getting a laptop riser and separate keyboard and mouse and finally – encourage each child to learn to type.

**(Culled from www.candp-s.com/familysafety)*