Acceptable Use of IT Policy for Pupils

Danes Hill School

February 2019

Contents

Clause

Appendix

1 Aims

1.1 This is the IT acceptable use policy for pupils of Danes Hill School (**School**).

1.2 The aims of this policy are as follows:

1.2.1 to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

1.2.2 to safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

(a) exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

(b) the sharing of personal data, including images;

(c) inappropriate online contact or conduct; and

(d) cyberbullying and other forms of abuse.

1.2.3 to minimise the risk of harm to the assets and reputation of the School;

1.2.4 to help pupils take responsibility for their own safe use of technology;

1.2.5 to ensure that pupils use technology safely and securely and are aware of both external and peer-to-peer risks when using technology; and

1.2.6 to prevent the unnecessary criminalisation of pupils.

2 Scope and application

2.1 This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

2.2 This policy applies to pupils accessing the School's technology whether on or off School premises, or using their own or others' technology in a way which affects the welfare of pupils or any member of the School community or where the culture or reputation of the School is put at risk.

2.3 Parents are encouraged to read this policy with their child. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

3 Regulatory framework

3.1 This policy has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 *Statutory framework for the Early Years Foundation Stage* (DfE, March 2017);

3.1.3 Education and Skills Act 2008;

3.1.4 Childcare Act 2006;

3.1.5 Data Protection Act 2018 and General Data Protection Regulation (GDPR) and

3.1.6 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2018);

3.2.2 Preventing and tackling bullying (DfE, July 2017);

3.2.3 Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety, August 2016);

3.2.4 Advice and guidance: How can we stop prejudice-based bullying in schools? (Equality and Human Rights Commission);

3.2.5 Sexual violence and sexual harassment between children in schools and colleges (DfE, May 2018); and

3.2.6 Searching, screening and confiscation: advice for schools (DfE, January 2018).

3.3 The following School policies, procedures and resource materials are relevant to this policy:

3.3.1 behaviour policy;

3.3.2 anti-bullying policy;

3.3.3 e-safety policy;]

3.3.4 safeguarding and child protection policy and procedures;

3.3.5 risk assessment policy

3.3.6 privacy notice for pupils

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request

4.3 A copy of the policy is available for inspection from the Deputy Headmaster or Bursar during the School day.

4.4 This policy can be made available in large print or other accessible format if required.

5 Definitions

5.1 Where the following words or phrases are used in this policy:

5.1.1 References to the **Proprietor** are references to Governing Body.

5.2 The School will take a wide and purposive approach to considering what falls within the meaning of **technology**. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

5.2.1 the internet;

5.2.2 email;

5.2.3 mobile phones and smartphones;

5.2.4 desktops, laptops, netbooks, tablets / phablets;

5.2.5 personal music players;

5.2.6 devices with the capability for recording and / or storing still or moving images;

5.2.7 social networking, micro blogging and other interactive websites;

5.2.8 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;

5.2.9 webcams, video hosting sites (such as YouTube);

5.2.10 gaming sites;

5.2.11 virtual learning environments such as Danes Hill VLE;

5.2.12 e-learning platforms;

5.2.13 SMART boards; and

5.2.14 other photographic or electronic equipment e.g. GoPro devices.

6 Responsibility statement and allocation of tasks

6.1 The Proprietor has overall responsibility for all matters which are the subject of this policy.

6.2 To ensure the efficient discharge of its responsibilities under this policy, the Proprietor has allocated the following tasks:

Task	**Allocated to**	**When / frequency of review**
Keeping the policy up to date and compliant with the law and best practice	Deputy Headmaster (also the Privacy Officer) and Bursar	As required
Monitoring the use of technology across the School, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change	Deputy Headmaster (also the Privacy Officer) and Bursar	As required

Task	Allocated to	When / frequency of review
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	Deputy Headmaster (also the Privacy Officer) and Bursar	As required
Online safety	Designated Safeguarding Lead	As required
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	Deputy Headmaster (also the Privacy Officer) and Bursar	As required
Seeking input from interested groups (such as pupils, staff, parents) to consider improvements to the School's processes under the policy	Deputy Headmaster (also the Privacy Officer) and Bursar	As required
Formal annual review	Proprietor	Annually

7 Safe use of technology

7.1 We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

7.2 The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. The safe use of technology is integral to the School's curriculum. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

7.3 Pupils may find the following resources helpful in keeping themselves safe online:

7.3.1 http://www.thinkuknow.co.uk/

7.3.2 http://www.childnet.com/young-people

7.3.3 https://www.saferinternet.org.uk/advice-centre/young-people

7.3.4 https://www.disrespectnobody.co.uk/

7.3.5 http://www.safetynetkids.org.uk/

7.3.6 http://www.childline.org.uk/Pages/Home.aspx

7.4 Please see the School's e-safety policy for further information about the School's online safety strategy.

8 Internet and email

8.1 The School provides internet access and an email system to pupils to support their academic progress and development.

8.2 Pupils may only access the School's network when given specific permission to do so. All pupils will receive guidance on the use of the School's internet and email systems. If a pupil is unsure about whether he / she is doing the right thing, he / she must seek assistance from a member of staff.

8.3 For the protection of all pupils, their use of email and of the internet will be monitored by the School. Pupils should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

9 School rules

9.1 Pupils **must** comply with the following rules and principles:

9.1.1 access and security (Appendix 1);

9.1.2 use of internet and email (Appendix 2);

9.1.3 use of mobile electronic devices (Appendix 3); and

9.1.4 photographs and images (including "sexting") (Appendix 4).

9.2 The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

9.3 These principles and rules apply to all use of technology.

10 Procedures

10.1 Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils he / she should talk to a teacher about it as soon as possible.

10.2 Any misuse of technology by pupils will be dealt with under the School's behaviour policy and where safeguarding concerns are raised, under the safeguarding and child protection and safeguarding policy and procedures.

10.3 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's anti-bullying policy. If a pupil thinks that he / she might have been bullied or that another person is being bullied, he / she should talk to a teacher about it as soon as possible. See the School's anti-bullying policy for further information about cyberbullying and e-safety, including useful resources.

10.4 The Designated Safeguarding Lead takes lead responsibility within the School for safeguarding and child protection, including online safety. In any cases giving rise to

safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures].

10.5 If a pupil is worried about something that he / she has seen on the internet, or on any electronic device, including on another person's electronic device, he / she must tell a teacher about it as soon as possible.

10.6 In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

10.7 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead, the Headmaster and the Deputy Head who will record the matter centrally.

11 Sanctions

11.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Proprietor has authorised the Headmaster to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's behaviour policy including, in the most serious cases, exclusion. But any action taken will be appropriate to the offence.

11.2 Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy and the School's behaviour policy (see the behaviour policy for the School's policy on the searching and confiscation of electronic devices).

11.3 If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

11.4 The School reserves the right to charge a pupil or his / her parents for any costs incurred to the School as a result of a breach of this policy.

12 Training

12.1 The School ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that staff and volunteers understand what is expected of them by this policy and have the necessary knowledge and skills to carry out their roles.

12.2 The level and frequency of training depends on role of the individual member of staff.

12.3 The School maintains written records of all staff training.

13 Risk assessment

13.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

13.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as

behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

13.3 The Headmaster has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

13.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Deputy Head and Bursar who have/has been properly trained in, and tasked with, carrying out the particular assessment.

14 Record keeping

14.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

14.2 All serious incidents involving the use of technology will be logged centrally by the Designated Safeguarding Lead and the Deputy Headmaster

14.3 The records created in accordance with this policy may contain personal data. The School has a number of privacy notices which explain how the School will use personal data about pupils and parents. The privacy notices are published on the School's website. In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this policy. This includes the School's data protection policy.

15 Version control

Date of adoption of this policy	February 2019
Date for next review of this policy	February 2020
Policy owner (members of SMT)	Deputy Head, DSL, Bursar
Policy owner (Proprietor)	Governing Body

Appendix 1 Access and security

1 Access to the internet from the School's computers and network must be for educational purposes only. You must not use the School's facilities or network for personal, social or non-educational use without the express, prior consent of a member of staff.

2 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

3 No laptop or other mobile electronic device may be connected to the School network without the consent of a member of the ICT department. Pupils are responsible for making sure that any device inclusive of personal computers, tablets, and storage devices that have access at any time to the Danes Hill network have up to date virus protection at all times. Permission will not be given if the device is not using a locking system requiring a suitable password or code to access it.

4 The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

5 Passwords protect the School's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.

6 You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher or contact Head of ICT Services

7 You must not attempt to access or share information about others. To do so may breach data protection legislation and laws relating to confidentiality.

8 The School has a firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or Head of ICT Services

9 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter.

10 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to Head of ICT Services before opening the attachment or downloading the material.

11 You must not disable or uninstall any anti-virus software on the School's computers.

12 The use of location services represents a risk to the personal safety of pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

Appendix 2 Use of the internet and email

1 The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

Use of the internet

2 No pupil is to be granted access to the School's internet without a member of staff present.

3 You must use the School's computer system for educational purposes only and are not permitted to access interactive or networking without the express, prior consent of a member of staff.

4 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

5 You must not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by the Head of ICT.

6 You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

7 You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

8 You must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

9 You must not bring the School into disrepute through your use of the internet.

Use of email

10 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail through the School's network. This will be unnecessary as you are provided with your own personal email account for School purposes.

11 You must use your School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

12 Email should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in an email which is not appropriate to be published generally or which you believe the Headmaster and / or your parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone you did not intend.

13 You must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material you must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

14 Trivial messages and jokes should not be sent or forwarded through the School's email system. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the School's network to suffer delays and / or damage.

15 All correspondence from your School email account must contain the School's disclaimer.

16 You must not read anyone else's emails without their consent.

Appendix 3 Use of mobile electronic devices

1 **Mobile electronic device** includes but is not limited to mobile phones, smart watches, smartphones, tablets, laptops and MP3 players.

2 Mobile phones and other mobile electronic devices must be switched off (and not just on silent mode) and kept in bags during School hours, including at break times and between lessons. Use of such devices is only permitted during School hours with the express permission of a member of staff.

3 The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet using any mobile electronic device while you are on School premises or otherwise in the care of the School is strictly prohibited at all times and is only permitted with the express permission of a member of staff.

4 The use of mobile phones during the School day will not be necessary. In emergencies, you may request to use the School telephone. Should your parents wish to contact you in an emergency, they will telephone the School office and a message will be relayed promptly.

5 You must not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Headmaster in writing.

6 You must not communicate with staff using a mobile phone (or other mobile electronic device) except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

7 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's anti-bullying policy and behaviour policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's child protection and safeguarding policy and procedures).

8 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the School's behaviour policy on the searching of electronic devices. You may also be prevented from bringing a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Head.

9 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

Appendix 4 Photographs and images

1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

2 You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image. If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted and the device will be delivered to the police, as stated in paragraph 11.3 of this policy.

3 You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

4 The posting of images which in the reasonable opinion of the Headmaster is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

5 **Sexting**

5.1 **Sexting** means the taking and sending or posting of images or videos of a sexual or indecent nature of you or another pupil, usually through mobile picture messages or webcams over the internet.

5.2 Sexting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

5.3 Sexting may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image. Even if you are not prosecuted, this may result in information being stored on your police record, which may prevent you from doing certain jobs in the future.

5.4 The police may seize any devices which they believe may have been used for sexting. If the police find that a device contains inappropriate images, they are unlikely to return it to you.

5.5 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

5.6 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

5.7 Even if you don't share images yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

5.8 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures).

5.9 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.