DANES HILL SCHOOL

STRONG & SAGACIOUS

Date: 30 April 2021

Review Date: September 2021

Author: Head of ICT Academic

E-Safety Policy

Contents

Section A

Introduction

Historically, the Internet Policy has resided in the domain of the ICT department and considered, in the main part, pupils accessing the Internet. ICT systems have developed rapidly over the past ten years resulting in more varied and advanced opportunities for communication using mobile devices, for social networking and instant messaging. For the purpose of this document the terms Information, Technology and Communication may be referred to as ICT or Technology.

These advancements, coupled with a broader use of such technologies, have resulted in the issue of child safety with regards to technology becoming a whole school issue. It falls under the banner of Safeguarding. As such this document has been reviewed in order to fulfil the school's responsibilities under **Keep Children Safe in Education 2020.**

It is the purpose of this ***E-Safety Policy*** to address the issues relating to child safety in conjunction with ICT and to define policy, ensuring maximum benefit whilst reducing risks where possible.

This policy incorporates the following policies and references the following additional documents:

Safeguarding and Child Protection Policy,
Preventing and Tackling Bullying Advice,

Staff Handbook and Staff Code of Conduct,
Data Protection Policy
Privacy Policy for Parents and Pupils

To ensure that Danes Hill School remains current with all issues relating to e-safety, an E-Safety Coordinator has been appointed in accordance with government guidance. The Designated Safeguarding Lead is the E-Safety Coordinator whose function is to:

1. Promote discussion and develop strategies to further the issue of e-safety.
2. Ensure that the culture of e-safety is part of Safeguarding and that it remains a whole school issue.
3. Develop policies that seek to ensure safe use of ICT throughout the school and at home.
4. Liaise between the various stakeholders in the school relating to wider issues of child welfare, whole school management and curriculum. These can include the:
    a. Head
    b. Deputy Head
    c. Assistant Head Academic
    d. Head teacher of Bevendean
    e. Head of Academic ICT
    f. Head of ICT Services
    g. Governing body
    h. Heads of Section and Heads of Year
    i. ICT teaching staff
    j. Parent community

5. Train staff and parents in the issues of e-safety

This policy has been created in consultation with the above bodies (a-g) and made aware to all others in the school community.

This policy document is reviewed regularly to encompass emerging technologies and to respond to changes in whole school policy and government guidance.

The Head of ICT will attend on a regular basis the Optimus Education Online Safeguarding Conference. This is vital and keeps the school abreast of the latest developments.

Uses and Benefits of Information and Communication Technology

At Danes Hill we are very aware of both the potential benefits and dangers of technology and ICT. This policy has been developed in an attempt to minimise the danger and maximise the potential.

The purpose of ICT in the school is to:

1. Through referencing Keeping Children Safe in Education 2019 we aim to provide a safe environment for pupils to develop their knowledge of technology now and for future use both inside and outside of the school site.
2. Comply with the requirements of the National Curriculum in England "which expects pupils to be digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world"

3. To provide a website that showcases the work of the school, reflects our place in the community and provides easily accessible and relevant information about current teaching topics and educational matters to staff, pupils, parents and the wider community.

4. Allow children and staff to access the Internet via a Web Browser which leads them directly to the school Intranet site. When a user follows a link outside the Intranet and onto the Internet, the user is then authenticated using their Windows network user account. All traffic is logged.

5. Train pupils for use of Internet technologies (including use of the Danes Hill VLE, website browsing, Email and the use of other communication devices) outside the protected environment of the school.

6. Provide the Staff with a maintained VLE site which provides:

    a. A storage area for All SafeGuarding Policies and Guidance notices, Medical information and Guidance and The Staff Handbook and Code of Conduct
    b. Announcements area

The Staff communication area (currently the VLE) is published in a protected area inaccessible to pupils when they log on. It is therefore vital, that staff do not leave a classroom when they are still logged on to a PC. Locking the computer is secure but only advised when the teacher is returning to that workstation before it is needed by another colleague.

Summary of Electronic Systems in Place

School Network

School access is, presently, via a computer network distributed over both campuses but chiefly used in the 3 ICT suites (one at Bevendean and 2 on the main site), iPads and other wireless devices. Every academic teaching classroom and teacher's office is also connected to the network

Internet Access

Internet access is controlled and only users with a current network account can access the internet. Logs exist of all the users who access the system and provides list of sites visited. All pupils in Bevendean, Years 2-8 and all staff have access to the Internet via the proxy server. Logs are kept for at least 12 months and if an issue is suspected the log files can be accessed and inspected.

Firewall

Internet traffic in and out of the school is controlled by a firewall whose purpose is to prevent malicious acts perpetrated by unauthorised users. The firewall is used to control the types of activities used in school such as blocking access to Social media, Networking sites and Forums that are both undesirable and not of critical educational benefit.

Filtering and Network Usage

The school uses a filtering system to manage the sites that are accessible by both staff and students

Where a site is accessed but is deemed unacceptable the Head of ICT should be informed as soon as possible to instigate an investigation as to any consequences.

If a site is blocked that is deemed educational by a member of staff who has viewed the site elsewhere, the technical; team at school can be contacted for them to consider unblocking the site.

The sites accessed that are flagged as blocked are reviewed periodically by the Systems Manager and appropriate action taken where necessary. As with all systems, effectiveness is continually evaluated and the entire filtering, logging and monitoring system is due for a review in September.

Monitoring Software

Impero Education Pro is installed on all Windows computers within the school. Impero encompasses of a range of classroom monitoring software, device management and network management. Its online safety functionality safeguards students using keyword detection libraries based on bullying, homophobia, grooming and sexting, suicide, eating disorders and self-harm, violence and radicalisation. In the event of Impero alerting the department to unsafe activity online, the Head, Deputy Head and DSL and Head of ICT will be alerted.

Email

Danes Hill School uses Microsoft Office 365 including the One drive and Email software. The Email platform can be accessed on the school site as well as remotely accessed by staff from home via secure SSL logon to school system. Every user on the network has access to an Email account. Staff can use the Email in a manner appropriate to their other professional levels of conduct and in accordance with the ***Staff Information Systems Code of Conduct*** document (see Acceptable Use Policy sections).

Wireless Local Area Networks (WLAN)

Currently the school uses wireless technologies throughout both sites. This Wireless access is a managed solution and access is controlled as with the main network.

Danes Hill VLE

The school VLE (Virtual Learning Environment) is a controlled and safe platform that allows a protected area for pupils to continue their learning outside of the confines of the classroom. It aims to provide an opportunity for teachers to provide their classes with alternative resources that are not always available through traditional means, such as the watching of videos for homework.

The VLE has an internal messaging system which allows for communication between pupils and teachers and between teachers and teachers. The system does not allow for pupil to pupil communication or for them to communicate outside of the school community. The messaging system has a built in filtering system that checks against a word bank and then reports to the class teacher and VLE administrator any words contained in conversations.

The system is hosted by an outside company which complies with current UK Data protection legislation.

E-Learning Sites

The school subscribes to a number of E-Learning platforms that are used by pupils in all phases of the school. They are all closed areas that do not allow any communication within or outside of the school community.
The sites all comply with the current UK Data protection legislation.
As of the start of the 2020 Academic year the following sites are used by Danes Hill pupils:
Math Wizz,
Purple Mash,
Doddle learn,
Pearson Active Learn,
Dynamic learning.

In addition to these sites the school subscribes to a number of online assessment packages that pupils access inside and outside of the school site. The sites do not allow the pupils to see any personal information referring to other pupils.

Section B

Constituent Policies

The E-Safety policy is a wide-ranging document which encompasses all aspects of ICT in the school. For clarity and easy reference, this policy section has been subdivided into smaller statements that can be digested more readily.

1. Access to ICT facilities

Pupils are only allowed into an ICT suite when a member of staff is there. Under no circumstances are pupils to log on to the system without a member of staff present. In Bevendean pupils use common credentials to access the system such as their class name or year group. In years 2-3 , pupils will log on to the system with an individual username but a common password for that year. At the beginning of Year 4, pupils will be allowed to change the common password to one of their own choice. This can be reset by the system admin but not viewed.

2. Internet Research

Gathering information using the Internet remains one of the main uses of ICT but inherent in this are issues relating to content and suitability. How the pupils use the World Wide Web depends upon their age and is summarized as follows:

Bevendean:
Pupils can use a website that has been opened up by the class teacher for use with the Promethean or SMART interactive whiteboard. This is done under the strict supervision of the class teacher or teaching assistant. Currently, pupils using the ICT suite do not have access to the internet but the teacher can display a website using the projector. The suite is for pupils to use software to learn ICT skills as well as to enhance their learning for other subjects.

Years 2-5:
Given the potential access to electronic media and the internet our children are able gain outside of the school, it is now felt that educating our pupils to use search engines such as Google responsibility is a vital skill. Pupils are closely supervised when using it and are to use within defined parameters.

Year 6-8:
Pupils in Years 6-8 will be allowed to access search engines such as Google as well as using encyclopaedia sites such as Wikipedia.

When a class is searching for information, the member of staff must be extremely vigilant. They must not take the opportunity to use the time while pupils are searching to perform other tasks on the teacher's PC. It is vital that staff help the pupils with their research.

It is important to teach pupils how to search successfully for information. During ICT lessons, pupils will be taught all the relevant skills needed to access information as swiftly as possible and then how to access the relevant information for their project work.

3. *E-mail*

Email addresses have been supplied to all teaching and support staff. These are addresses supplied by school and follow the pattern of *initialsurname*@daneshill.surrey.sch.uk As the school email address contains the school domain name, all users are regularly reminded that anything they write therefore reflects upon the school and should always be carefully considered so that it does not bring the school into disrepute.

Due to the messaging facility on the VLE, pupils do not have a school email account they are still however taught to use email as part of the ICT programmes of study – which include rules for safety and how to send sensible, polite letters which obey the same rules as formal letter writing.

4. *Social Networking Sites, Forums and Blogging Sites*

Access to any social networking sites such as Facebook are strictly forbidden and as such they are blocked within the school for both pupils and staff.

However, whilst it is recognised that the majority of our pupils are not old enough to use most Social media, we need to ensure that they are made aware of how to use it safely if they do use it (See section C). However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networkin g applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst pro viding a framework of good practice. They apply to all members of staff at the school.
The purpose of the policy is to:

- Protect the school from legal risks
- Ensure that the reputation of the school, its staff and governors is protected
- Safeguard all children
- Ensure that any users are able clearly to distinguish where information provided via social med ia is legitimately representative of the school.

5. *Removable Media*

Pupils are discouraged from bringing work from home on USB Drives. When essential, it can be but permission and supervision must be provided the teacher. This is to ensure that there are no viruses in the files and also check for pupils bringing in undesirable content.

Members of staff who are confident in using the Virus Scanning system may also perform the check at the teacher's PC.

6. *YouTube*

Staff are allowed to access YouTube videos. Staff are asked to preview each video for suitability beforehand. Pupils are not allowed to access YouTube videos.

7. *Danes Hill VLE*

The school VLE (Virtual Learning Environment) is a controlled and safe platform that allows a protected area for pupils to continue their learning outside of the confines of the classroom. It aims to provide an opportunity for teachers to provide their classes with alternative resources that are not always available through traditional means, such as the watching of videos for homework.

The VLE has an internal messaging system which allows for communication between pupils and teachers and between teachers and teachers. The system does not allow for pupil to pupil communication or for them to communicate outside of the school community. The messaging system has a built in filtering system that checks against a word bank and then reports to the class teacher and VLE administrator any words contain in conversations.

Pupils are reminded at the beginning of the year and periodically how they should use the system and how they should address teachers when messaging them. They are reminded that their messages can be viewed and that its use falls under the school's behaviour system.

The system is hosted by an outside company which complies with current UK Data protection legislation.

8. *E-Learning Sites*

The school subscribes to a number of E-Learning platforms that are used by pupils in all phases of the school. They are all closed areas that do not allow any communication within or outside of the school community.
The sites all comply with the current UK Data protection legislation.

9. *School Website*

The school website will reflect the school – its standards, work and ethics and will be carefully presented to ensure that the school is well represented. It will be a forum for presenting exemplary work from the pupils. It will raise motivation – and thus standards, by presenting children with a real audience for their work. It will be a showcase for the school and a point of contact with the parents and local community.

The majority of the school website pages are openly accessible to the entire Internet community. Certain pages have been deemed as either only relevant to the school community or contain data that might compromise the security of pupils, staff and the school e.g. Email addresses and the newsletter. In these cases, access to the pages are through a common username and password that is made known, periodically, to the school community. Content is added by a team and monitoring is done by the Marketing Manager, the Head and the Deputy Head.

The following conditions are to be considered before publishing material:

a. No child is identified by name.
b. No child known to be at risk is pictured on the website.
c. All pictures of children are published as small sized, compressed jpegs of gifs so that they may not be downloaded and used for dubious purposes.
d. If any complaint is received from a parent, the picture or information concerned will be removed immediately without argument.
e. Parents are given the opportunity to refuse permission for their child's photograph to appear on the Website by contacting the Deputy Head directly.
f. Children's work published to the website must reflect the standards of the school.
g. The School Website will only publish school contact details and school email addresses.
h. Home information, individual email identities and personal details will not be published.
i. Content from other people that is copyright (including logos) is not knowingly used without obtaining permission.
j. Links to other sites are carefully considered to make sure that they are relevant, helpful and suitable; and are tested at intervals to ensure their integrity. If any complaint is received about a link being either unobtainable or unsuitable, it is investigated as soon as possible to maintain the standard of the website the school in the best light and to ensure their safety.

10. Mobile Phones and all Internet enabled devices

The school policy remains that no pupil is allowed to bring in a mobile phones, internet enabled devices or digital cameras to school or on any trips.

Staff are not permitted to make/receive calls/texts during contact time with children. Staff are not at any time permitted to use recording equipment on their mobile phones, e.g. to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras or iPads.

Cyberbullying

The following are extracts from the paper on Cyberbullying (found as an appendix at the end of this policy). It outlines the school's response to issues of cyberbullying and recognises the problems associated with electronic forms of bullying.

Aims and Implications for Danes Hill School with regards to Cyberbullying:
It is vital that action is taken to secure the following aims:

1. Danes Hill School is kept aware of changes in digital technologies.
2. To ensure that Danes Hill School continues to adopt a policy of encouraging pupils to tell when they feel threatened in any way.
3. To educate pupils via ICT, Citizenship and PHSE lessons and through visits from outside agencies in strategies in dealing with cyberbullying, as well as all aspects of online safety and where to go if in need of help.
4. To make pupils and staff aware of the legal issues of digital harassment.
5. To be aware that, as with other abuse issues that occur outside school, cyberbullying can have its roots in school. There must also be an awareness that the effects of cyberbullying can be

manifest in school and that the school is the common ground for contact between victims and bullies

6. To provide clear channels of disclosure, namely the Designated Safeguarding Lead (DSL) but also an awareness that all staff will listen and be sympathetic.
7. Ensure that all staff are made aware of the categories of cyberbullying and the consequences to the pupils.
8. Ensure that policies relating to mobile phones in school (currently banned) are reviewed continually and balanced against those welfare policy decisions relating to school trips and unaccompanied travel to and from school.
9. To monitor, where at all possible, the use of electronic communication systems when accessed on the school premises i.e. Email and Website usage.
10. To ensure that parents are kept informed of developing issues and the school policies regarding Internet Safety and bullying and Internet Safety are updated accordingly.
11. To ensure that parents know what steps to take if they suspect their child is being cyberbullied.

Amendments to School Policy on Bullying

1. Danes Hill School recognises that whilst the acts of cyberbullying rarely occur on the school premises, it is our responsibility to:
    a. Be aware of all methods of cyberbullying.
    b. Educate our pupils and parents in how to avoid cyberbullying situations
    c. Encourage pupils to take appropriate action and know to whom they can approach.
2. Danes Hill School recognises the additional opportunities that electronic technologies present to those with a mind to bully and that ALL electronic means of bullying is unacceptable.
3. Where the matter of bullying is covered in the curriculum, all aspects of cyberbullying are to be addressed.
4. All staff are to read the cyberbullying document (included in the staff handbook and policy section of the M Drive) and acquaint themselves with the types of cyberbullying and the legal consequences.
5. Where an incident is discovered and deemed severe, Danes Hill School may inform the appropriate outside authority including:
    a. Internet Service Providers
    b. Mobile Telephone Providers
    c. Police
    d. Childline 0800 1111
    e. CEOPS 0870 000 3344
    f. Social Services (LADO)

11. Sexting (Youth Produced Sexual Imagery)

In the event of a sexting incident, staff are instructed not to look at the contents, move or download the contents or take any action other than to inform the Head, Deputy Head and Designated Safeguarding Lead immediately.

They will contact the Surrey Police Child Protection Unit, who will take appropriate action.

This process is designed to safeguard any children involved.

Pupils within Years 7 and 8 will receive training on sexting within their annual E-safety talk given by Childnet in January of each academic year.

12. Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism. The school's safeguarding policy, available on the school Intranet and in school, covers Radicalisation and Extremism. Although serious incidents involving radicalisation have not occurred at Danes Hill to date, it is important for staff to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Designated Safeguarding Lead). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and students. Impero Education Pro (installed on all Windows computers within the school) uses keyword detection libraries which include radicalisation.
All staff have undertaken recognised online training in awareness and understanding of the Prevent duty.

13. Copyright and Plagiarism

As with all published material, issues of copyright and plagiarism exist as do laws governing the use and distribution of said materials.

Danes Hill School will ensure that staff are made aware of copyright issues relating to Internet derived materials in the **Information Systems Code of Conduct for Staff** document.

Pupils will be made aware of the issues of copyright and plagiarism. The will be given strategies in ICT lessons to critically analyse Internet derived material for accuracy and how to acknowledge information sources.

Danes Hill School

E-Safeguarding Personal Data and Security

Policy and Best Practice

P Sarginson
Updated 22nd November 2020
Next review September 2021

Data Security

The school network contains vast amounts of sensitive data about our children. By law we need to abide by the Data Protection Act. This, not only controls what is stored and for how long, but also how our data is handled, backed up and transferred.

The ICO (Information Commissioner's Office) summarises that organisations must:

- only collect information that you need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as you need, and only for as long as you need it; and
- allow the subject of the information to see it on request.

The Data Protection Act 1998 requires all organisations to secure any personal data they hold. This covers data held both electronically and on paper.

What constitutes Personal Data?

Personal data is any combination of data items that identifies an individual and gives specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth, behaviour and assessment records. The Data Protection Act 1998 specifies additional data items as 'sensitive personal data', this includes medical records, criminal convictions and ethnic origin.

- Formatted Excel reports contain full names and class data and as such are regarded as Personal Data. These must now be encrypted to carry off site.
- A Word document containing a class set of reports is not generally regarded as Personal Data but as a safeguard, it is recommended that only First names are used.
- It is the responsibility of the Danes Hill School System Manager (currently RivaNet) to ensure that all Personal Data is saved and backed up successfully.
- Any member of staff needing to learn how to encrypt data are to liaise with the ICT Technical staff to ensure that this is done successfully.
- Trips booklets and other paper copies containing personal data also apply and must be disposed of in a secure manner.

To ensure Danes Hill School remains compliant with current strategies adopted in the public and private sectors, staff are asked to adhere to the following:

Danes Hill School – Data Protection Policy and Best Practice

1. No personal data shall be taken from Danes Hill School unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, IPads, netbooks, external hard disks, memory sticks and Personal Digital Assistants (PDAs) & other removable media.

2. Any member of staff, when aware of the loss of Personal Data shall immediately report any loss of personal data to the Head.

3. Remote access is granted to all staff for home access. To maintain data security, staff must:

a. Ensure they use a strong password which is changed at least once a term. This is soon to become mandatory and a necessary action to access the system. A strong password has letters and numbers as well as a combination of upper and lower case letters.
b. No other member of the household is to use the system.
c. Ensure that when using the remote access system at home, they should never leave the system unattended or visible to any other member of the household.

4. Any formatted Excel spreadsheet taken from SIMS is to be encrypted before emailing to home or placing on removable media.

5. Personal Data for report writing stored on a home system will be deleted within 1 month of the report deadline.

6. Passwords are to be changed once a term. At the moment this is recommended practice but in due course, staff will be forced to change their password once a specified time period has elapsed. This is common practice in the public and private sectors.

Hard Copy Data Protection

There are many documents that are printed out that are valuable to staff but contain personal data. This includes, but not limited to, trips booklets, exam or test data, form or set lists.

Policy and Best Practice:

1. Trips booklets are to be handed back to the trip leader at the end. They will then be taken to the Deputy Head's office and added to financial documents for shredding.

2. All other hard copy material containing Personal Data on children are to be kept only for as long as needed and then shredded. Wastepaper bins or using the recycling system is not deemed as secure disposal.

Backups and Disposal of Hard Disks

The ICT Technical department is responsible for backing up all personal data as well as all user created files. It is also responsible for the secure disposal of hardware.

Policy and Best Practice:

1. Data is to be backed up at regular intervals to a secure location. As Danes Hill is fortunate to have a campus structure, data can be backed up to a geographically different location within the school, negating the need to take backups off site. In the case of the SIMS database, this is backed up using a Cloud-based system that guarantees data protection.

2. When old hardware is ready for disposal, the school will adopt one of two strategies with regard to the safe disposal of the Hard Disk.
   a. Remove and physically destroy the Hard Disk in house before the remainder of the system is sent to a recognised recycling firm and obtain a WEEE certificate.

b. Send the completed system to a firm that is accredited for data removal to an acceptable level and will also provide a Waste Electrical and Electronic Equipment (WEEE) certificate.

Essential ICT Information
for all Danes Hill School Staff

Preface

This booklet is not designed, in any way, to replace the E-Safely policy or any other policy currently published. It exists to provide staff with a very quick reference guide for the most crucial aspects of ICT at Danes Hill School and is to be regarded as the essential, 'must know' information. Much of this booklet is common sense and some might seem restrictive but it is essential that no member of staff is given an opportunity to put a child at risk. Much of the advice is given to protect staff and the school in the event of a wrongful accusation by a child or parent.

Section A: Cameras and Phones

1. No smartphone is to be used to take photos of pupils under any circumstances.
2. Mobile phones are not to be used in front of children except in an emergency situation.
3. Games and PE staff are *never* to bring out their phone in a changing situation.
4. Staff are not to use personal digital cameras for any reason. The school will provide cameras, stored in strategic areas, for use.
5. Staff are not to take photos of pupils in costumes/outfits that might compromise the modesty of the child e.g. swimming costumes.

Section B: General use of ICT systems

1. Staff should log off a PC when they leave the classroom. (Lock is acceptable if it can be guaranteed that they will return prior to another staff member needing that PC)
2. Staff should ensure that a projector is not on when sensitive information is viewed on a PC.
3. Staff are to be aware that their school Email account contains the school name and represents the reputation of the school. It is to be used professionally at all times.
4. No pupil is to be granted access to the ICT facilities without a member of staff present
5. No pupil is allowed to log on to any home, personal account such as Email or Cloud storage.
6. Only pupils in the Middle and Upper School are to be allowed to search using Google.

Section C: Social Networking and Email

1. Staff are free to receive Emails or messages (on the VLE) of work from pupils but ONLY to their school account. Under no circumstances is a personal Email to be given to pupils.
2. Staff responding to a work Email from a child should reply courteously, but briefly and not in a familiar manner.
3. No member of staff should be a 'friend' or be in any other contact with present pupils ***or past pupils under 18yrs,*** on social media.
4. Pupils are forbidden to upload photos containing the image of a member of staff on any social networking site.
5. School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at Danes Hill School.
6. Any communication received from children on any personal social media sites must be reported to the Designated Safe Guarding Lead.
7. If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
8. Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
9. All email communication between staff and members of the school community on school business must be made from an official school email account.
10. Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.
11. Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
12. Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts.

Section C

E-Safety Education Programme including communication of policy and Virtual Learning Environments

The use of technology has become a significant component of many safeguarding issues, including, but not limited to, sexual exploitation, radicalisation and sexual predation. Danes Hill strives to provide an effective approach to online safety which both protects and educates the school community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

For any policy to be effective, it must be successfully communicated to all sections of the school such as pupils, staff and parents. It is vital that all staff are aware of the policies and adhere strictly to them to provide consistency throughout the school which is so important when dealing with issues of child safety and welfare. Pupils will be given guidance and limitations of use as part of their ICT lessons which is backed up by all class teachers in PSHEE lessons.

E-Safety Education Programme

Bevendean:
In Bevendean, this will be addressed primarily by their class teacher as part general classroom rules. When pupils use the ICT suite for the first time, they will be given instructions on good behaviour. This will be reinforced with a poster in the suite. Bevendean (Year 1) will use the Childnet resource: Smartie the Penguin with an emphasis on 'telling'. The ICT Coordinator will lead a whole Bevendean assembly at the beginning of each Academic year on the subject of E-safety.

Year 1 will receive a talk by Childnet in January each year as part of their visit each year.

Lower School:
On the main site it is the task of the ICT teacher to reinforce good practice and in Year 2 and 3 to introduce the use of the Internet to the classes. A simple acceptable use sheet will be discussed in ICT lessons. The following website is used to introduce children to the potential benefits of the Internet:

http://www.teachingideas.co.uk/welcome/internet/page1.htm

Year 2 will watch a short cartoon called Child Focus "E-safety" and focuses on who too talk to if they are not happy.

Year 3 will look at online resources in ICT lessons. The ICT teacher will show a short age appropriate cartoon produced by Child Exploitation and Online Protection Command (CEOP) on using the internet called "Hectors World". Year 3 will focus on Safe Searching and foster an awareness that online friends are essentially strangers. They will examine the CBBC safe surfing rules.

Middle School:

The middle school Acceptable Use Policy (AUP) will be introduced in ICT lessons which is backed up by posters in classrooms. ICT lessons pick up on Internet Safety again in Year 5 with a course based on the SMART rules outlined in the Childnet International Website:

http://www.childnet-int.org/kia/primary/smartadventure

Pupils create an internet safety poster on the SMART rules. These rules go home to parents to involve them with aspects of internet safety.

Year 4 will follow on from the Year 3 safety information. In ICT lessons, they will take time to examine the CEOP – 'Animal Magic' cartoon and discuss the content.

Year 5 will view the CEOP'S cartoon 'Cara and Winston' and discuss it connection with the SMART rules, created by Childnet, which will be followed up in PSHEEE lessons. They have a page in their homework diary that addresses the AUP and the Smart Rules.

Upper School:
Year 6 This is the age at which pupils begin to be more vulnerable to the negative aspects of the Internet. ICT lessons will reiterate the themes of safe surfing, chat rooms IM and social networking sites,

Pupils will also visit the BBC Newsround site to refresh themselves of key advice:

http://news.bbc.co.uk/cbbcnews/hi/find_out/guides/tech/safe_surfing/newsid_1607000/1607213.stm

They will focus on issues relating to social networking making a particular reference to Facebook. Even though the age of consent for Facebook is 13, we are aware that many children have an account and it is vital that they learn 'in advance' the ways of maintaining privacy and altering settings and a common sense approach to what is inadvisable to post. They will watch the CEOPS video 'Jigsaw' and discuss the issues surrounding the story.

Year 7 will address the issues around cyberbullying. They will watch the BBC video "Newsround Caught in the Web"and discuss the issues surrounding the story. In PSHEEE, pupils will view the 'Let's fight it together' film and discuss the issues of how to react to being bullied electronically. They will also be given a leaflet produced by the school on Cyberbullying.

Year 8 will concentrate on the issues surrounding posting or sending various forms of personal information and in particular an awareness of their Digital Footprint. Naturally, this will include Sexting and pupils will see an excellent film that cover, not only the issues, but how to cope if a mistake is made. This will be delivered by the presenter from Childnet. Year 8 classes will also watch a CEOPS video and discuss the issues surrounding the story.

In addition to this programme of study, we invite Childnet to talk to the pupils, annually. Childnet are also invited in to give a most comprehensive talk to staff and parents each year and we hope that you will find the time to attend.

Main school will attend an assembly and participate in activities linked to the Safer Internet day on or around the first Tuesday in February each year.

All pupils in Years 1 – 8 are given a talk by Childnet International every year, they address the issues of Internet Safety and how to avoid risks (next visit planned for January 2020).

Staff:

Staff are trained annually via structured INSET on matters of Internet Safety and safeguarding, especially where there is a major change in policy or new guidance is introduced. Staff are required to attend the talk after school by Childnet International

New staff are given an introduction to the ICT systems as part of their induction sessions and those currently undergoing the QTS course have Internet Safety built in to their programme of study.

This policy (as all others) is available in hard copy on request from the Head of ICT and electronically on the Staff network.

Periodically, (so as to include recent additions to the common room) staff are required to read the **Information Systems Code of Conduct** document and sign a form to state that this has been read and the terms within agreed to.

Parents:

The role of parents in matters of Internet safety is vital for our children to remain safe when online. The existence of this policy is made aware to parents in the **Student Acceptable ICT Use Policy** and can be viewed at any time on request to the Head of Academic ICT or the Head master's secretary.

Periodically, parents are invited to meetings where matters relating to Internet safety are addressed (next visit planned for January 2021). The Childnet International and CEOP (ThinkUKnow) websites contain much relevant information:

http://www.childnet-int.org/kia/parents/cd/

http://www.childnet-int.org/downloads/blog_leaflet.pdf

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

Parents are able to contact the Head of ICT via Email in the first instance, to discuss any matter relating to ICT and their child.

It is the school policy to require parents to sign an Acceptable Use agreement at the start of their child's schooling at Danes Hill, which includes internet access. It is made explicit in the letter to parents that the Internet is widely used at school and that this includes the use of the internet offsite as well.

If a child joins the school at any time in the school year other than the start, **Student Acceptable ICT Use Policy** will be included in their starting pack

Danes Hill School

Leatherhead Road OXSHOTT Surrey KT22 0JG

Student IT Acceptable Use Policy

Danes Hill School provides access to computing equipment for its students; enabling the use of technology in everyday learning across many subjects. The use of IT equipment is monitored and supervised by the Danes Hill School teaching and administration staff. Before a student can use any equipment it is expected that the parents/guardians agree to the Student IT Acceptable Use Policy of the school.

The Agreement: -

I agree that the student named below should: -

- Follow the guidelines of behaviour and language presented in any Danes Hill School policy when using Danes Hill School's computers.
- Be responsible for all actions on the computer network and the Internet.
- Protect the privacy of other students. Not read, change, delete, copy or use the computer files of another person without the person's permission.
- Refrain from installing any program without written consent and review by the network administrator.
- Not access any file or insert a CD, flash drive or other removable media into any Danes Hill School computer without review for viral infection by the network administrator.
- Refrain from attempting to access any computer system or equipment at Danes Hill School by trying to learn passwords, or defeat security measures instituted by staff members.
- Not upload, download, or bring inappropriate or offensive material into the school. This would include, but not be limited to, any profane, vulgar, or sexually explicit material or material that is violent in content. Materials that reflect racism, bigotry, hatred, or that are in opposition to the standards of the school philosophy are considered inappropriate.
- Not knowingly upload, download, or bring any file containing or linking a virus, or worm.
- Recognize the value of hardware, software, and all computer related materials; not misuse or abuse any of these items. Refrain from behaviour that might result in damage of any kind to equipment or software.
- Understand that direct access to the Internet is limited to use for a specific purpose, at the request of specific teachers, and is under the supervision of a faculty member. Not abuse the privilege of such use and restrict Internet access to the assignment given.
- Keep passwords to themselves and never use another's password.
- Respect copyright laws by not downloading or attempting to download copyrighted material. Avoid plagiarism, as defined as the use of another's words or idea as one's own.
- Refrain from behavior or activity that damages or disrupts the performance of the network.
- Report any misuse of the network to the computer teacher or administrator.
- Not bring a phone or internet enabled device to school or on any trips. (unless specifically agreed)
- I understand that the above also applies to the VLE and any Danes Hill e-learning sites that I may access from inside or outside of the school site.

Furthermore, I acknowledge that: -

- The school network is monitored and the network administrators have full access to all emails and files to make sure the network is used in a suitable manner.
- Any Danes Hill IT equipment is to remain in school unless specific circumstances have agreed by management.
- If IT equipment is taken off the school site, then it is the Parent/Guardians responsibility to make sure the device is kept safe. This includes but not limited to physical damage, theft, loss and breaches of software policy highlighted earlier in this agreement.
- If any physical damage, theft, loss or breaches of software policy is to occur then the IT administrators must be made aware as soon as possible and you may be liable to a fee.

The Parent/Guardian accepts that any breach of this policy may result in access being taken away from the student and future access will be reviewed. Breach of the policy may also result in disciplinary action. This policy remains in force for any student at Danes Hill School and for the duration they are a student.

As parent or guardian, I accept the terms of this policy on behalf of myself and the named child:

Student Name:_____

Parent/Guardian Name:_____

Parent Guardian Signature:_____ Date:_____

.

Virtual Learning Environments

A virtual learning environment, or VLE as it is known, is an Internet-based system that allows users – in our case, pupils and staff – to engage in educational activities away from the classroom. These systems allow schools to offer 'anytime, anywhere' learning which the government has strongly endorsed.

Lower and Middle VLE

Launched in September 2017, Danes Hill uses the provider e-Schools for its VLE. The VLE is hosted on the e-Schools own servers. There is no opportunity for communication between pupils on the VLE, only between pupils and teachers.

The Lower and Middle school classes use Purple Mash. They all have secure, individual accounts to access the activities through a Single Sign On authentication. It is envisaged that more class extension work will be given to pupils from this site.

Pupils are taught how to use both the VLE and the Purple Mash site in ICT lessons and staff explain that all work produced online is visible to us at school. The Head of ICT provides email support for parents.

Upper School VLE

Launched in September 2017, Danes Hill uses the provider e-Schools for its VLE. The VLE is hosted on the e-Schools own servers. There is no opportunity for communication between pupils on the VLE, only between pupils and teachers.

All pupils will be trained in ICT lessons prior to using the VLE and will be reminded of the following conditions:

1. Access to the site is only to be done using their own username and password.
2. All site access and activity is logged and these logs will be viewed periodically but the Head of ICT.
3. Actions taken on the VLE are to be regarded as public and monitored by members of staff.
4. Any breach of these conditions and any misuse of the VLE will result in the immediate blocking of access to the site and referral, if necessary, to the Deputy Head.

Pupils' activity will be checked periodically and log files can be produced for any given time period.

Section D

Digital Learning Agreements

Bevendean

Computer Rules

These rules help me to stay safe on the Computer

I will only use the computer when my teacher allows me.

I will only do the tasks that my teacher has given me to do.

I can use a webpage that my teacher has opened for me.

If I get stuck I will ask for help.

When I have free choice, I will only choose from the icons on the desktop.

Lower School

Think before you click

S 	I will always ask permission before using the computer.
A 	I will only click on icons and links when I know they are safe.
F 	I will only send friendly and polite messages.
E 	If I see something I don't like on a screen, I will always tell an adult.

Lower School Digital Learning Agreement

Middle School

Middle School Digital Learning Agreement

These rules will keep me safe and help me to be fair to others.

- I will always ask permission before using the computer.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission.
- I am aware that some websites, videos, games and social networks have age restrictions and I should respect this.
- I will only message people I know, or a responsible adult has approved.
- All messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher or responsible adult.
- I will not bring in a mobile phone or Internet-enabled device to school.

Middle School SMART Rules for Internet Safety

KEEPING SAFE ONLINE

S afe (or Secret) – Always keep your name, address, mobile phone no. and password private – it's like giving out the keys to your home.

M eeting in real life someone you met on the Internet can be dangerous. Never arrange to meet up with someone that you only know online. If anyone asks you to meet up, discuss this with a trusted adult.

A ccepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

R eliable. Remember, someone online may be lying and not be who they say they are. Stick to public areas in Chat rooms and if you feel uncomfortable – get out! Never trust 1 website take a look at 2 or more.

T ell your parent or carer if someone or something makes you feel uncomfortable or worried.

Visit the SMART crew site:

http://www.childnet-int.org/kia/primary/smartadventure/chapter1.aspx

Upper School

Upper School Digital Learning Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my Internet use.
2. I will not bring files into school that can harm the school network.
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my year group.
6. I will only e-mail or contact people I know, or those approved as part of learning activities.
7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
9. I will not give personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
12. I am aware that some websites, games, music, videos and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
14. The internet at school is filtered to prevent unpleasant sites appearing. At home my access may not be filtered, so I will take extra care.
15. I will endeavour to create a positive digital footprint and will respect the rights of others to do this as well.
16. I will not bring in a mobile phone or Internet-enabled device to school.

Section E

Reporting, Sanctions and Review

Reporting:

1. Disclosures

If a child discloses to a member of staff a problem of any description the same approach must be taken as with any child protection issue. In the first instance the teacher will listen and use common sense judgements to deal with the situation. If it is deemed that the issue warrants further help use the following as guidance.

If the child is in need of some technical know-how or the issue is minor, and the member of staff feels ill-equipped to deal with the situation, then the Head of ICT is always available for these queries from pupils and staff alike. Please refrain from giving promises that the issue will be sorted instantly as some might take a bit more research or investigation.

A child might disclose that they have been involved in any activity/action/contact online that is concerning them e.g. feeling groomed, inappropriate contact online, sexting or the invitation to send photos to an online contact. In this situation, it is vital to report it to the Designated Safeguarding Lead (DSL).

2. Access to Internet Resources at School

In the event of a pupil accessing a website that is of questionable content, or receiving an unsolicited Email (spam) the Head of ICT is to be informed in the first instance.

If the content has in any small way disturbed or unsettled the child, the Designated Safeguarding Lead is to be notified. The Head or Deputy Head will then be contacted as soon as possible and an action plan drawn up which may involve:

1. Blocking the site
2. Gathering evidence of site visited and how the site was opened.
3. Contacting the parents
4. Contacting the ISP (Easynet)
5. Contacting the Police or social services if the matter is of a criminal or illegal nature.

The primary outcome is to ensure that this instance will not happen in the future and all reasonable steps employed to carry out additional protection if deemed appropriate.

Sanctions

Pupils:

Where a child is deemed to have breached the acceptable use policy, the incident must be reported in the first instance to the Head of ICT. Depending on the severity of the incident, one or more of the following sanctions may be carried out:

1. Verbal reprimand
2. Minus given
3. Loss of free time (morning break)
4. Referral to Deputy Head
5. Referral to Head

If the Head deems the activity serious, the school's behaviour policy will take effect and appropriate discipline administered.

If the activity is such that it is deemed illegal or criminal as defined by law such as the Computer Misuse Act 1990 (see Appendix 4) the school reserves the right to contact the police. In this event the parents must have been contacted prior to any contact with the police.

For cases of cyberbullying outside of school, they will be dealt with on an individual basis by the Head of Section or the Deputy Head.

Staff:

In the event of staff misuse of the system, the incident must be dealt with by the Head or the Deputy Head. If the activity is such that it is deemed illegal or criminal as defined by a law such as the Computer Misuse Act 1990 (see Appendix 4) the school reserves the right to contact the police. The staff disciplinary procedure will then be invoked by the Head.

Review

This document is regarded as both a statement of policy and as a working handbook. The contents are subject to frequent change, based on whole school policy changes, technological advances and changes in government guidelines.

The E-safety Coordinator and the Designated Safeguarding Lead, will endeavour to remain abreast of current thinking on the subject and attend courses and conferences where possible.