COGNITA
TEACHING EXCELLENCE

NIHIL VIRTUTI INVIUM

DOWNSEND
SCHOOL

ONLINE SAFETY POLICY

ONLINE SAFETY

1.0 Introduction

1.1 Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment. Throughout the school the teaching and learning process emphasises the importance of being a responsible 'digital citizen' and encourages students and staff to use web based technology and social media responsibly with consideration for others.

1.2 I.C.T. covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of I.C.T. within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

1.3 Whilst exciting and beneficial both in and out of the context of education, much I.C.T., particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

1.4 At Downsend School, we understand the responsibility to educate our pupils on Online Safety issues; 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, in and beyond the context of the classroom.

1.5 Both this policy and the Acceptable Use Agreement (for all Staff and Pupils) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards and digital video equipment); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players).

1.6 We define Online Safety as:-

- ensuring student Internet use and access is appropriate and controlled.
- preventing misuse of Internet connected devices.
- ensuring students are educated on the risks carried with Internet use and how to minimise and deal with those risks.

- providing students with knowledge and resources to make decisions to ensure their safety online

1.7 Our core principles for Online Safety are:-

- The Internet and Internet connected devices provide a rich resource for supporting teaching and learning.
- Our policies seek to educate and inform students and the school community on the safe and prudent use of Internet resources
- We take a whole school, consistent approach to Online Safety, recognising that all staff should be involved and clear on their role in ensuring Online Safety education.
- Online Safety is subject to clear reporting routines
- We recognise the need for regular training and ensure at least one member of staff takes accredited training and has a higher level of expertise.
- Our policy reflects current practice and is regularly reviewed and updated by the Lead Team and communicated to all staff.
- Online Safety is addressed within the curriculum at all ages.
- Technology in school is monitored to ensure it offers a safe access point to the Internet
- This policy should complement other school policies, in particular safeguarding policy; staff acceptable Internet and device use; data protection, anti-bullying or similar policies and student / pupils sign an Acceptable Use of Technology Agreement in advance of using the school/their own digital devices.
- The Online Safety policy is dated with a review date and a named member of staff has responsibility for ensuring it is reviewed and updated on an annual basis

2.0 Roles & Responsibilities

2.1 As Online Safety is an important aspect of strategic leadership within the school, the Heads of School and Headmaster have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

2.2 The named Online Safety Officers in our school are: Mr Karl Newland (Upper School) & Mrs Claire Kirkham

2.3 All members of the school community have been made aware of who holds this post. It is the role of the Online Safety officers to keep abreast of current issues and guidance through organisations such as Surrey LEA, CEOP (Child Exploitation and Online Protection) and Childnet.

2.4 The Senior Leadership Team are updated by the Online Safety officers and Head of ICT. Through appropriate INSET, staff have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

2.5 This policy, supported by the school's acceptable use agreements for Staff and Pupils (Appendices 1 and 2), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy.

2.6 Each academic year staff receive information and/or training on Online Safety issues. All staff are reminded of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see Appendix 5). New staff will receive information on the school's acceptable use policy as part of their induction. All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

3.0 Online Safety in the Curriculum

3.1 I.C.T. and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety. In Key Stage 2, pupils learn about Internet safety as part of their work using sites such as Miss Dorothy materials (www.missdorothy.com and Hector's World (http://www.thinkuknow.co.uk/5_7/hectorsworld/). Additional resources, including those from CEOP and Childnet International may be used across the school e.g. The Adventures of Kara, Winston and the SMART Crew, and the Cyber Café.

3.2 Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum (subsumed within the P.S.H.E. curriculum) and in assemblies across the school pupils are made aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP using the report abuse button. Digital citizenship evenings are run for parents & staff to inform and update on the changing face of social media and online gaming issues.

3.3 Internet skills are taught as part of the I.C.T. scheme of work including: Analysing data and asking questions and using complex searches. The development of Internet skills is also an ongoing process, as children use the Internet for research purposes across the school and in most areas of the curriculum. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will be taught the importance of cross-checking information before accepting its accuracy; to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3.4 We endeavour to embed Online Safety messages across the curriculum whenever the Internet and/or related technologies are used.

4.0 Password Security

4.1 Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords (for the network and e-mails and the website which are not shared with anyone. Pupils have individual passwords to access the pupil portal and their own profiles, which they are expected to keep secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded, via network reminder messages, of the need for password security. Short-term supply teachers should see the Head of ICT/ICT technicians in order to be provided with a temporary username and password to enable them to access the necessary 'SMART' Board resources and other electronic resources to deliver that day's lessons.

4.2 Users who think their password may have been compromised or discovered by others should ask the Head of I.C.T. to reset their password.

4.3 Staff must also ensure that workstations are locked (using Ctrl, Alt, Delete) when they are left unattended (i.e. during P.E. lessons and at playtimes and lunchtimes.) All users need to ensure that all browser windows are closed down fully after logging to ensure that other people using the computer cannot access their account, using their identity.

5.0 Data Security

5.1 The accessing and appropriate use of school data is something that Downsend School takes very seriously. Data can only be accessed and used on school computers or laptops,or devices that have secure permission rights. Staff are aware they must only use their personal devices for accessing relevant school, class or pupil data. The school will purchase password protected/encrypted memory sticks when teachers are required to work with personal data at home (for example, when writing end of year reports).

5.2 The school network is backed up securely by the Head of ICT/ICT technicians.

6.0 Initial Considerations

6.1 The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the school network is logged and the logs are randomly but regularly monitored by the ICT technicians and Head of ICT. Whenever any inappropriate use is detected it will be followed up. The school will supervise access to Internet resources (where reasonable) through the school's fixed and mobile Digital technology. Staff will preview any recommended sites before use. Younger pupils should be directed to a specific website or a selection of preapproved websites and avoid using search engines. When working with older pupils, an appropriate and safe search engine should be used, e.g. Primary School Safe Search (www.primaryt.co.uk/pupils.html). Raw image searches are discouraged when working with pupils. If Internet research is set for home learning, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

6.2 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

6.3 Upon request, web-based activity can be monitored and recorded. School Internet access is controlled through the web filtering service. In addition, our school also manages some bespoke web filtering which is the responsibility of the Head of ICT, working with our support services at Cognita Head Office.

6.4 Downsend School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

6.5 Staff and pupils are aware that school based e-mail and Internet activity can be monitored and explored further if required. The school does not allow pupils access to Internet logs, and uses management control tools for controlling and monitoring workstations. If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the Online Safety officer. The offending URL will be reported to the Head of ICT.

6.6 Sophos Anti-Virus protection is set to automatically update on all school machines. This is the responsibility of the Head of ICT/ICT technicians working with our support services at Head Office. In addition staff laptops and home computers can also be protected by Sophos Anti-Virus as agreed by the Head of ICT.

6.7 Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head of I.C.T. If there are any issues related to viruses or anti-virus software, the Head of I.C.T. Co-ordinator should be informed using the I.C.T. 'Issues' book , which is kept in the staffroom and monitored on a daily basis by the Head of ICT.

7.0 Managing other Web-based technologies

7.1 The Internet, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

7.2 At present, the school denies access to social networking sites to pupils within school. Many of our children will access these sites from home, so all pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are. They are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online. Where relevant they will be advised to use 'avatars' instead.

7.3 Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home telephone numbers, school details, instant messaging/e-mail address, specific hobbies/interests). They will be advised to use nicknames, and to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Pupils are encouraged to be wary about publishing specific and detailed private thoughts online. They are asked to report any incidents of bullying to the school. Our pupils will be introduced to a variety of Web tools within the safe context of the ICT suite and curriculum.

7.4 Where a member of staff uses social networking sites outside of school, he/she should avoid any information that could compromise his/her professional integrity, and be fully conversant with the security arrangements for the site in use. Strong passwords should be used and security settings should be applied so that he/she controls all access to his/her profile.

8.0 Mobile technologies

8.1 Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and 'Smart' phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and potential misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Downsend manages the use of these devices in the following ways so that users exploit them appropriately.

8.2 Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device.

Pupils are not allowed to bring mobile phones to school. However, in Years **6-8**, parents may apply for specific permission for their children to bring their mobile phones to school where they are needed for use outside of school e.g. when walking home from school. Where permission has been granted by the Head of School, pupils must hand the phone-clearly labelled with pupil name & class – to the member of staff on Turret duty/or handed in to the School Office upon arrival at school.

The school is not responsible for the loss, damage or theft of any personal digital device.

Permission must be sought before any image or sound recordings are made on these devices by any member of the school community. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

8.3 School provided Mobile devices (including phones)

Permission from the relevant Head of School must be sought before any image or sound recordings are made on devices provided by the school by any member of the school community.

Where the school provides mobile technologies such as phones and laptops for offsite visits and trips, only these devices should be used.

9.0 Managing e-mail

ONLINE SAFETY

9.1 The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools and other external links, on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good 'netiquette' including appropriate salutation. In order to be ICT literate pupils must have experienced sending and receiving e-mails.

9.2 The school gives all staff their own account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced.

9.3 The Staff account should be used for all school business. E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending e-mails to external organisations are advised to cc. the relevant Head of School. E-mails sent to pupils as part of an e-mail topic or other work relating to school keep a copy in their sent items folder. Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

9.4 Pupils may only use school approved on the school system and only under direct teacher supervision for educational purposes.

9.5 All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments (see Appendix 4.

9.6 Pupils must immediately tell a teacher/ trusted adult if they receive an offensive message by phone, text or email and should keep the offending message(s) as evidence. Staff must inform the Online Safety officer and relevant Head of School if they receive an offensive e-mail.

10.0 Safe Use of Images / Film

10.1 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, may be misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Ideally, staff should not use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on field trips. However with the express permission of the Headmaster, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

10.2 Consent of adults who work at the school

Permission to use images of staff on the school website is sought before publishing.

10.3 Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web-site Manager, has authority to upload to the website.

10.4 Storage of Images

Images/ films of children are stored on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Head Teacher. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/Learning Platforms.

10.5 Photographs or images

By signing the Acceptance Form or agreeing to these terms and conditions the Parents consent to the School obtaining and using photographs or images of the Pupil for:

- use in the School's promotional material such as the prospectus, the website or social media;
- press and media purposes;
- educational purposes as part of the curriculum or extra-curricular activities.
- If a parent does not want the Pupil's photograph or image to appear in any of the School's promotional material they must make sure the Pupil knows this and must write immediately to the Admissions Secretary requesting an acknowledgement of their letter.

ONLINE SAFETY

10.6 Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the Headmaster and Business Manager. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in school other than for special projects e.g. bird box images from the school garden which may then be streamed to the web. They are only ever used for specific learning purposes, and never using images of children or adults. Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

10.7 Video Conferencing

Permission is sought from parents and carers if their children are involved in video conferences internally or with end-points outside of the school. All pupils are supervised by a member of staff when video conferencing. The school will keep a record of instances of video conferences, including date, time and participants. Approval from the Headmaster is sought prior to all video conferences within school.

Conferencing equipment will not be set to auto-answer and will be switched on for scheduled and approved conferences only. No part of any video conference will be recorded in any medium without the written consent of those taking part.

Users should be aware that participants in conferences offered by third party organisations may not be CRB checked. Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

11.0 Misuse and Infringements

11.1 Complaints relating to Online Safety should be made to the Online Safety officer or Head of School. Incidents should be logged (Appendix 4) and process should be followed (Appendix 5).

11.2 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety officer.

11.3 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety officer. Depending on the seriousness of the offence; investigation by the relevant Head of School or Head Teacher will take place followed by suspension, possibly leading to dismissal and involvement of police for very serious offences Users are made aware of sanctions relating to the misuse or misconduct by school's policy on disciplinary procedures.

12.0 Equal Opportunities

12.1 The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's Online Safety rules.

ONLINE SAFETY

12.2 Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

12.3 Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities will be planned and well managed for these children and young people.

13.0 Parental Involvement

13.1 We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school. Downsend has run targeted information evenings, focus groups, INSET and assemblies on Online Safety and we consult and discuss Online Safety with parents/carers and seek to promote a wide understanding of the benefits related to I.C.T. and associated risks.

13.2 Parents/carers and pupils are actively encouraged to contribute to the school Online Safety policy. They are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website).

13.3 The school disseminates information to parents relating to Online Safety where appropriate in the form of:

- Posters
- Downsend Website/Parent/pupil portal
- Downsend Times Newsletter items

14.0 Procedure for Writing and Reviewing this Policy

14.1 On an ongoing basis, staff are encouraged to discuss with the Online Safety officer any issue of Online Safety that concerns them.

14.2 This policy will be reviewed every twelve months and consideration will be given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

14.3 This policy has been read, amended and approved by the Headmaster on 1 October 2016

15.0 Other Associated Policies & Procedures

- Safeguarding Children including Child Protection Procedures;
- Health & Safety;
- Safer Recruitment;
- Staff Handbook;
- Central Record of Recruitment & Vetting Checks;
- Compliments & Complaints Procedure;

- Data Protection;
- Anti-bullying;
- Staff discipline, conduct and grievance, procedures for addressing; and
- Whistle-blowing.