**Policy Last Reviewed: Sept 2018 KH**
**Next Review Due: Sept 2019 by KH**

# Denstone College

# Digital-Safety Policy

## Computing and ICT in the curriculum

Technology has transformed the process of teaching and learning at Denstone College. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All classrooms are equipped with interactive whiteboards or smart boards. There are 5 ICT suites in the school and pupils may use the machines there and in the library for private study. All the boarding houses are equipped with computers and network points.

All pupils are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution. Some sites that appear to be serious, impartial, historical sites are actually a façade for a variety of propaganda. Some free, on-line encyclopaedias do not evaluate or screen the material posted on them.

## The role of technology in pupils' lives

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, together with Bluetooth-enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging) services (like Twitter), to Skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms, online gaming sites, social networking sites (such as Bebo, Facebook and MySpace) and video sharing sites (such as YouTube). More recently sites such as Snap Chat and Instagram have increased in popularity.

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role to teach the pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. Pupils also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

Digital-Safety

Digital-Safety covers all aspects of pupils engaging with ICT where there is potential risk involved. Areas covered include:

- Cyber Bullying
- Access to the internet and inappropriate content
- Sexting
- Creating/sharing videos and images
- Using social media sites and understanding the potential dangers of membership e.g. sexual exploitation, grooming, abuse
- Blogging
- Mobile phones
- Online gambling
- Online gaming
- Spam, phishing, pharming
- Viruses and Malware
- Radicalisation and extremism

Role of the Digital-Safety Team

Due to the nature of Digital-Safety and the pace with which this landscape changes, a Digital-Safety team exists at the School. Chaired by the Director of IT this team meets on a regular basis each term and consists of the following members:

| | |
|---|---|
| Director of IT | Shelly Burrows |
| Deputy Head Pastoral & Designated Safeguarding Lead | Karenann Hood |
| Management of PSHE programme | Kathy Swords |
| Deputy DSL | Richard Neal |
| Designated Safeguarding Lead | Angela Smith |

The team is responsible for the co-ordination and delivery of the Digital-Safety programme across the School encompassing pupils, staff, parents and other relevant parties.

The team will ensure all staff receive training in Digital-Safety issues, as part of the college INSET programme and that all year groups in the school are educated in the digital risks and the reasons why they need to behave responsibly online.

A Digital-Safety folder is available on the I drive (I:\IT\Digital Safety) which will house key resources.

The Digital Safety Team will also use free self-evaluation tools such as 360safe.org.uk to review online safety practices and procedures.

Role of the technical staff

With the rapid explosion in technology of pupil access to personal devices, the blocking and barring of sites is no longer adequate. The pupils need to be educated to understand why they need to behave responsibly if they are to protect themselves. The technical staff have a key role in maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the college's hardware system, data and for training the teaching and administrative staff in the use of ICT. They monitor the use of the internet and will report inappropriate use to the Senior Master.

The technical staff set up internet permission sets for each pupil depending on their Year Group and whether they board. As a pupil progresses through the years' wider access is granted but all activity is closely managed and monitored. This has been greatly improved with the installation of Smoothwall a sophisticated web filtering software that enables tracking of a user name across all devices linked to the school network. It also enables a more refined set up of blocked websites and apps to be set up and allows the setup of automated reports to be generated daily to the safeguarding team based on a user's attempt to gain access to a blocked website. The safeguarding team monitor such use for trends and patterns.

Sophos is also used as the school's antivirus software to ensure the College's network and equipment is protected from virus attacks.

All activity on the network is closely monitored by the technical and safeguarding teams and pupils and staff alike are made aware of this. The Smoothwall filtering system provides a daily alert to the safeguarding team who monitor any concerns flagged and follow them up as appropriate.

Role of the Child Protection Team

Digital-Safety is a child protection and general safeguarding issue. Three members of the Safeguarding team sit on the Digital Safety Team. They have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices and work closely with the Staffordshire Safeguarding Children's Board (SSCB) and other agencies in promoting a culture of responsible use of technology, consistent with the ethos of Denstone College.

Role of the Governing Body

The governing body have a named governor, Jane Dickson, whose role it is to ensure that the College has effective safeguarding policies and procedures.

Misuse: Statement of policy

The College will not tolerate any illegal material, and will always report illegal activity to the police and/or the Staffordshire Child Safeguarding Board (SCSB). If it is discovered that a pupil is at risk as a consequence of online activity, assistance may be sought from the Child Exploitation and Online Protection Unit (CEOP).

In addition, it has now been recognised that some types of harassing, threatening behaviour or communication could be deemed a criminal offence. Under the Malicious Communications Act of 1988, any person who sends an electronic communication which conveys a message which is indecent,

grossly offensive, a threat, or information which is false and known or believed to be false by the sender, is guilty of an offence if their purpose in sending the communication was to cause distress or anxiety to the recipient.

The College will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with the anti-bullying policy.

Involvement with parents and guardians

The College works closely with parents and guardians in promoting a culture of Digital-Safety. The College will always contact parents if there are any concerns about a pupil's behaviour in this area, and parents are encouraged to share any concerns with the College. It is recognised that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. Discussion evenings for parents are arranged with an outside specialist advises about the potential hazards of technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. Parents have the legal responsibility to ensure that they and their child/children understand how to use technology safely.

All pupils and parents are asked to sign up to the 'Pupil Responsible use of Devices, Digital Sites and Content' policy. This policy, written for the pupil, sets out the do's and don'ts of using ICT in a responsible manner. This information is captured in ISAMs to ensure all pupils have signed the acceptance form and is updated on a regular basis. Due to the nature and pace of technological change, pupils are asked to sign a new form as and when new measures emerge.

In addition, as part of a calendar of events in this area, a series of evening events and communications aimed at parents and guardians will be organised each academic year. These events will be used to educate and inform.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not be used during lessons or formal school time unless specifically authorised by a member of staff or unless for a serious emergency. The sending of abusive or inappropriate text messages is forbidden. The use by students of cameras in mobile phones will be kept under review. Some games machines have internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

All pupils receive a College email account and there are policies in place to ensure staff and pupils only use College accounts for email communication. Staffs are also requested to set up email signatures which do not contain personal contact details e.g. personal mobile numbers.

In addition, a Digital Leaders group, led by pupils, meet each term to discuss the latest developments in technology from a pupil's perspective, share news on up and coming social sites and raise any concerns they have to do with Digital-Safety. Information and feedback from pupils can then be incorporated into the regular Digital-Safety meetings.

Handling Digital-Safety Misuse

Concerns of internet/digital misuse by pupils will be dealt with by relevant members of teaching staff (see Behaviour Policy). Any complaint about staff misuse must be referred to the Headmaster. Concerns of a child protection nature must be dealt with in accordance with the College's Safeguarding Policy.

Due to the rapid development and access to technology, 'virtual' or cyber bullying is on the increase and is not limited to College premises. This form of bullying can happen at any time during the day, has the potential to involve a wider audience and have more profound effects if left unreported. The Education Act of 2011 now states that when an electronic device has been seized by a member of staff, who has been formally authorised by the head teacher, the staff member can examine data or files, and delete these, where there is good reason to do so without parent/guardian consent. In a situation where a device has been seized and the staff member has reasonable grounds to suspect it contains evidence in relation to an offence, then they must give the device to a member for the safeguarding team without deleting the content. The safeguarding team will then decide whether the police are to be notified.

Communicating Digital-Safety: Introducing the Digital-Safety policy to pupils

As part of the induction process, all pupils receive ICT training and are made aware of computer facilities available to use when in school or offsite. In addition, they are asked to read and sign the Computer Use Acceptance policy when they are a new pupil at the school and each year thereafter. As part of the Year 1 to 3 Computing and ICT curriculum, Digital-Safety is incorporated into the scheme of work and a range of tutorials focus on this area during the academic year. The curriculum now also includes a lesson on online grooming with a focus on radicalisation and extremism. This subject is also covered in PSHE sessions where Middle and Senior School pupils are involved in discussions on this topic. Radicalisation and extremism are also included as topics in the GCSE religious education specification and this subject is mandatory for all middle school pupils. The CEOP link for pupils is also installed on all school computers.

The PSHE curriculum aims to build resilience in pupils to protect themselves and peers through education.

Staff and the Digital-Safety policy

All staff will be given the School Digital-Safety Policy and its importance explained. Staff must be informed that network, social media networks and internet traffic can be monitored and traced to the individual user. Staff who manage filtering systems or monitor ICT will follow clear procedures in the reporting of issues to SMT. Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship and adhere to the school's Data Protection Policy.

Enlisting parents' support

Parents' and guardians' attention will be drawn to the School Digital-Safety Policy in newsletters; the College will also provide Digital-Safety awareness evenings for parents. These events will be incorporated into the Digital-Safety calendar which can be found at the end of the policy and is updated annually. In addition, the parent portal page of the College website also includes useful digital safety links and information for parents.

## CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT DENSTONE COLLEGE

*"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim."* Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".

Digital-Safety is a whole school responsibility, and at Denstone College, the staff and pupils have adopted the following charter for the safe use of the internet inside the school:

### Cyber Bullying

- Cyber Bullying is the use of technology to harass, threaten, stalk, embarrass or otherwise intimidate someone. It may include use of email, social websites, online gaming sites or text messaging.
- Cyber Bullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The College's anti-bullying policy describes our procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe outside the college.
- All of our pupils will be treated equally; it is part of the ethos of Denstone College to promote considerate behaviour, and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

### Treating Other Users with Respect

- It is expected that pupils treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact.
- A degree of formality is expected in communications between staff and pupils, and staff and pupils would not normally communicate with each other by text or mobile phones. On Educational Visits or in the boarding community communication by mobile phone may be appropriate.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The Anti-bullying policy is published on the website. The College is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issue to a member of the pastoral staff.
- The use of cameras on mobile phones is not allowed in washing and changing areas. Careful thought needs to be given before using them in the bedrooms of boarding houses and during school trips.

Keeping the School Network Safe

- Certain sites are blocked by the filtering system and the ICT Department monitors pupils' use of the network.
- The ICT Department monitors email traffic and blocks most SPAM and certain attachments.
- All pupils are issued with their own personal school email address. Access is via personal LOGIN, which is password protected. Guidance is given on the reasons for always logging off and for keeping all passwords securely.
- Access to social networking sites is limited to boarders' free time.
- There is a strong anti-virus protection on the network, which is operated by the ICT Department.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- If staff or students discover an unsuitable site, it must be reported to the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Although the school network will be managed and appropriate web filtering software installed, students can still access the internet, social media and apps via personal mobile devices using 3G/4G. This is where educating the pupil in the responsible use of the internet is key and reinforced by the school through a number of channels including computer science lessons, PSHE, competitions and events.
- The Smoothwall web filtering software blocks 'categories' of sites and apps available on the internet. Should a teacher or pupil wish to use a blocked site for educational purposes, they will contact IT support with the web address they are trying to access and this can be investigated further. If suitable the specific website will be made available. The Smoothwall solution also generates reports containing users who have attempted to access blocked websites. These reports are sent to all members of the safeguarding team on a daily basis.

Social networking and personal publishing

The college will control access to social networking sites using the school network, and consider how to educate students in their safe use.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

Safe Use of Personal Electronic Equipment

- The guidance is that no one should put anything onto the web that they would not say to their grandmother!
- The PSHE programme offers guidance on the safe use of social networking sites and Cyber Bullying in PSHE lessons, which covers blocking and removing contacts from "buddy lists".
- PSHE lessons and tutorials include guidance on how pupils can identify the signs of an online-stalker, and what they should do if they are worried about being harassed or stalked online.

- Guidance is offered on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- Parents are encouraged to keep safe at home, by encrypting their home wireless network, not opening unknown attachments and reporting any illegal content. A mobile phone filter can be activated and nuisance callers can be blocked.
- The responsible use of Skype at College is encouraged but this is not officially supported software. Free video calls can provide boarders, particularly overseas boarders, with an effective way to maintain contact and relationships with their families and friends.

Considerate Use of Electronic Equipment

- Mobile phones, tablets, smart watches and other personal electronic devices should be switched off and stored securely during lessons. They may be used during free time.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

It is expected that all pupils adhere to this charter for the safe use of the internet. Sanctions may be imposed for the misuse, or attempted misuse of the Internet, mobile phones and other electronic devices.

Information Technology: Staff Code of Practice

All staff is expected to make appropriate use of College IT facilities. Inappropriate use including deliberately accessing pornographic or other offensive/unsuitable material will instigate the disciplinary procedure as listed in the Employment Manual: "Members of Staff are expected to act and perform their duties in a professional manner."

Security: Physical

The ICT rooms are protected by an alarm set each night when the room is closed by Senior School duty staff. In the event of problems during the working day the IT technician and IT Manager have details of the security provider and the necessary procedures (outside of normal working hours please contact the Maintenance Manager).

Security: Software

The network is protected by various passwords. In the event of unavailability of the IT technician or IT Manager please contact the Director of ICT.

Access

The rooms are available for use by members of staff at any time. The IT technician and Network Manager will be available from 8.45 am to 5:00 p.m. Monday to Friday. Pupils are not allowed to enter the ICT rooms without a member of staff in supervision and are not allowed to play games or consume food and drink in the rooms. A working atmosphere is encouraged. A timetable of allocated lessons is available on the Isams school software. Any member of staff may book the use of the rooms during unallocated periods by entering a booking on Room Bookings. Individual use is not encouraged for either staff, or pupils from outside the lesson, during taught ICT lessons. Access during non-taught lessons is at the discretion of the supervising member of staff. Problems with equipment or software should be reported to the IT technician or Network Manager.

Internet and e-mail
All pupils and staff have email addresses and can access the Internet.

2) Departmental and Other Facilities

There are other computers available for use throughout the College under the direction of the respective department heads.

Hardware & Software
All hardware and software for use in College must be authorised for use or purchased by the Bursar. The IT technician and IT Manager will install any additional software or hardware required.

Maintenance
Any requests for maintenance should be passed to the IT technician and IT Manager or in his absence the Operations Bursar.

Consumables
Ink cartridges, paper, discs etc. are available from the IT Technician or IT Manager and will be charged to the appropriate departmental budget.

Internet
Those departments with Internet provision must ensure that pupil use is consistent with the College IT policy.

3) SCR Facilities

All teaching staff has computing, Internet and E-mail facilities available in the SCR. Large attachments to emails should be avoided. Networked computers and black and white and colour printers are kept in the SCR for general use by teaching staff.

Staff Code of Conduct for Photographs and Videos (see Staff Code of Conduct for Digital Images and Videos Policy)

Permission required: When a new pupil joins the school, parents are asked via a data form to opt in to an agreement with the College to permit the use of their child's name and image for College and marketing purposes. Details of parents who have opted out can be found on ISAMS via reporting services. Good Practice where appropriate is that verbal permission will be obtained from pupils prior to taking and displaying photographs or video footage. The Second Master should be consulted if in doubt.

Guidance where permission obtained: Where permission has been obtained, the following should be considered:

- The purpose of the activity should be made clear as to what will happen to the photos.
- If the taking of pupil images is required, possession of these images must be justified.
- Images should not be made during one-to-one situations if at all possible.

- If an image is to be displayed in a place to which the public have access it should not display the pupil's name unless necessary.
- All images of children should be stored securely and only accessed by those authorised to do so. Those authorised include teachers, child safety officers and relevant support staff.

Appropriate material:

Children must not be exposed to inappropriate or indecent images. Inappropriate material, such as pornography, must not be brought to work and College property must not be used to access such material. Pupils are not permitted to have unauthorised access to College equipment and staff should keep computer passwords safe. In the situation where inappropriate material is discovered and is potentially illegal, the equipment must be isolated and contact with the designated Safeguarding Lead under the College's Safeguarding Procedures must be contacted immediately.

Links to Other School Policies: This policy needs to be read in conjunction with Computer use by Pupils, Pupil Email policy, Group Parental Communication policy, Data Protection policy, Code of Conduct for Photographs and Videos, Staff Email policy. Anti-bullying policy, Searching Pupil policy, Safeguarding policy.

Digital-Safety Calendar 2018 – 2019

| Term/Date | Event | Focus | Target Group |
|---|---|---|---|
| Michaelmas September | Digital-Safety Team Meeting | Planning of events | Staff Internal |
| Michaelmas September | New Pupils | New pupils to sign Pupil Computer Use form | New Pupils |
| Michaelmas September | School website / parent portal review | Update parent portal with new information where applicable | Parents |
| Michaelmas September | Digital Leaders Group Meeting | Pupil led technology group | Pupils |
| Michaelmas October | 360safe.org review | Self-evaluation of Online safety | Digital Safety Team |
| Michaelmas October | Junior School Curriculum | First 3 – 4 weeks of term focussed on digital safety | 1st Years, 2nd, 3rd Years |
| Michaelmas October | Parent Communication | Digital safety communication and distribution of Digital Parenting magazine | New parents to Denstone Existing parents |
| Michaelmas October | Tutorial | CEOP Exposed / Indecent Images | All year groups |

| | | | |
|---|---|---|---|
| | | Competition? | |
| Michaelmas October | Digital-Safety Team Meeting | Planning of events | Staff Internal |
| Michaelmas November | Digital Leaders Group meeting | Pupil led technology group | Pupils |
| Michaelmas December | Parent Communication pre-holiday | Safety Online | Parents |
| | | | |
| Lent | Digital Day – Karl Hopwood/House competition | School wide event to cover all year groups, staff and parents. Prep school also included. | Staff, pupils, parents, pre prep pupils (DCPS) |
| Lent February | UK Internet Safety week and Cultural Cup Competition | School focus | Pupils / link to cultural cup |
| Lent February | Tutoral Quiz | Digital Safety quiz | All pupils |
| Lent March | 15F | Pupil led event on their digital use | Pupils to deliver to staff |
| Lent March | PSHE Tutorial | Topic TBC | All Year groups |
| Lent March | Digital Leaders Group Meeting | Digital-Safety | All Year groups |
| | | | |
| Summer April | Digital-Safety Team Meeting | Planning of events | N/A |
| Summer May | Digital Leaders Group Meeting | Digital-Safety | All Year groups |
| Summer May | 15F | Pupil led event on their digital use | Pupils to deliver to staff |
| Summer May – June | Senior School Social Media Trawl | Search through social media targeting Senior School pupils – evidence gathering prior to UCAS discussions | Senior School |
| Summer June | Digital Leaders Group Meeting | Digital-Safety (regular agenda item) | All Year groups |
| Summer | Email with attachment – key digital safety messages | Digital-Safety top tips | Parents/Guardians |
| Summer | Prepare key message for Sept 2019 Tutor Groups | Key digital safety messages to be shared with tutors and tutees in week 3 | All pupils |

| | | | |
|---|---|---|---|
| | | or 4 of Michaelmas 2019. Appropriate key messages for each year group. | |

Future Events/Activities to Consider

- Digital Safety Conferences/training
- New parents email for digital safety
- Feedback from 360 safety online review