Policy Last Reviewed: August 2023
Next Review Due: August 2024

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 College and pupils may use the machines there and in the library for private study. In the Prep School pupils have use of 20 laptops for ICT lessons within the classroom and cross curricular ICT. Pre-Prep pupils also have use of 5 tablets. 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 on 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 Facebook) and video sharing sites (such as YouTube). More recently sites and apps such as SnapChat, TikTok 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

This policy has due regard to all matters outlined in Keeping Children Safe in Education 2022.

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, Deputy Head Pastoral, Deputy Head (Pupils), Head of Prep School, Head of PSHE & Wellbeing and members of the Safeguarding team.

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

The team will ensure all staff receive training in Digital-Safety issues, as part of the Denstone 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 Denstone 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 Deputy Head (Pupils) in the College and Head of Prep in the Prep school.

The technical staff set up internet permissions 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 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.

Malwarebytes is also used as the school's antivirus software to ensure the College's network and equipment is protected from virus and malware 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 Safeguarding Team

Digital-Safety is a child protection and general safeguarding issue. Four 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 Denstone College has effective safeguarding policies and procedures, she also sits on the Digital Safety Team.

Misuse: Statement of policy

Denstone 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.

Denstone 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

Denstone College works closely with parents and guardians in promoting a culture of Digital-Safety. Denstone 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. 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 to advise 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 in The Prep school are asked to sign a "Charter for the safe use of the internet" (Pupil Acceptable Use Agreement – Prep School) this outlines the expected behaviour towards the use of IT. This information is stored in the ICT Subject Handbook in Teams.
All pupils and parents in the College are asked to sign the 'Pupil Acceptable Use Agreement'. 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.

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 Phone are not allowed in the Prep School. In the Senior School 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 pupils 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 Denstone College email account and there are policies in place to ensure staff and pupils only use College accounts for email communication.

In addition, a Digital Leaders group, consisting of a group of pupils in the College, 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 Head or Head of Prep. Concerns of a child protection nature must be dealt with in accordance with Denstone 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 Denstone 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, 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

In the Prep School

The safe use of Technology is integral to the School's ICT curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices Technology is included in the educational programmes followed in the EYFS in the following ways:

(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

(b) children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology;

(c) children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies, PSHE and teaching pupils:

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

(b) to be critically aware of content they access online and guided to validate accuracy of information;

(c) how to recognise suspicious, bullying, radicalisation and extremist behaviour;

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

(e) the consequences of negative online behaviour; and

(f) how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat.

In the College

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 Pupil Acceptable Use Agreement when they are a new pupil at the school. As part of the 1st to 3rd Form Wellbeing programme, 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. Radicalisation and extremism are also included as topics in the GCSE religious education specification for those middle school pupils that have chosen the subject as an option. All pupils are encouraged to report any digital safety concerns or issues they may have to staff. The CEOP link for pupils is also installed on all school computers and the Pupil Voice facility is provided for the reporting of non-emergency issues or concerns.

The Wellbeing (PSHE) curriculum across the school 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 College'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 a Digital-Safety awareness evening 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:

Cyberbullying

- Cyberbullying 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.
- Cyberbullying 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 for pupils in the main school.
- 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 IT Support monitors pupils' use of the network.
- IT Support monitors email traffic and blocks most SPAM and certain attachments.
- All College 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, having strong unique passwords and the need to keep them securely.
- Access to social networking sites is age restricted and limited to outside of lesson times.
- There is a strong anti-virus protection on the network, which is operated by IT Support.
- 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 pupils discover an unsuitable site, it must be reported to the IT 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, pupils can still access the internet, social media and apps via personal mobile devices using 3G/4G/5G. 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 computing lessons, Wellbeing, tutor time, 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

Denstone College will control access to social networking sites using the school network, and consider how to educate pupils 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 Wellbeing and Computing programme offer guidance on the safe use of social networking sites and Cyber Bullying, which covers blocking and removing contacts.
- Wellbeing / Computing lessons and tutorials (Form time in the Prep School) 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 digital 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 video calling at the 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 personal devices and mobile phones

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the College.

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: *Anti-Bullying*, College *Behaviour*, and *Safeguarding*.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibilities for the loss, theft, damage or breach of security of such items on school premises
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt according to the behaviour policy.
- All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive or harmful.
- College pupils with mobile phones or tablets and other personal electronic devices should ensure they are 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.
- In the Prep school Mobile phones, ipods and other personal electronic devices are not allowed in school.

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 Acceptable Use Agreement

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

Security: Physical

The ICT rooms are protected by the building alarms set each night when the building is closed by duty staff. In the event of problems 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 IT.

Access

The rooms are available for use by members of staff at any time. Members of IT support 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 IT support.

Internet and e-mail

All College pupils and staff have email addresses and can access the Internet.

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 the College must be authorised for use by the IT manager, GDPR and Compliance Manager and purchased by the Bursar. IT support will install any additional software or hardware required once authorised.

Maintenance

Any requests for maintenance should be passed to IT support or in their absence the Bursar.

Consumables

Ink cartridges, paper, discs etc. are available from IT Support 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 Pupil Acceptable Use Agreement and the Charter for the safe use of the internet.

SCR Facilities in the Main school and The Prep

All teaching staff have access to computing, Internet and E-mail facilities available in the SCR, library and school provided laptops. Large attachments to emails should be avoided. Networked computers

and colour printers are kept in the SCR for general use by teaching staff.

Staff Code of Conduct for Photographs and Videos (see Staff Acceptable Use 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 Deputy Head Pastoral 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 Denstone College property must not be used to access such material. Pupils are not permitted to have unauthorised access to Denstone 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:

Pupil Acceptable Use Agreement

Staff Acceptable Use Agreement

Data Protection policy

Anti-bullying policy

Searching Pupil policy

Safeguarding policy.

Denstone College
Pupil Acceptable Use Agreement- Prep School

for the safe use of the Internet at the Prep

Technology is an important part of Denstone College life and beyond. Using ICT in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the ICT systems or to other users is important. This acceptable use agreement explains your responsibilities and sets out the principles we expect you to adhere to when using ICT at Denstone College and outside of Denstone College premises.

We agree to

- treat everyone online with the same good manners as we would when talking face to face
- only go 'online' when a member of staff is present and with his/her permission
- keep safe and private our 'log in' details, along with our names, addresses, passwords, mobile phone numbers and other personal details.
- only access sites which we know are suitable; if we are in doubt, we will ask the teacher
- only download material we know is suitable and appropriate; if we are in doubt, we shall ask a teacher
- report any worrying issue to a member of the pastoral staff.

Pupil's Agreement

I have read and understand the Pupil Charter

I understand this charter will be in place whilst a pupil at Denstone College Prep School.

Signed: **Date:**

Parental/Guardian Agreement

I have read, understood and shared with my child the Charter.

Signed: **Date:**

Denstone College
Pupil Acceptable Use Agreement- The College

Technology is an important part of Denstone College life and beyond. Using ICT in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the ICT systems or to other users is important. This acceptable use agreement explains your responsibilities and sets out the principles we expect you to adhere to when using ICT at Denstone College and outside of Denstone College premises.

Safety and Security

- I will use only my own login and password, which I will keep secret.
- I know that the College may check my computer files and may monitor the Internet sites I visit.
- I understand certain members of staff are authorised to look at the content of my electronic device should they suspect an offence has been committed. They do not need my or my parents'/guardian's consent to carry out such a search.
- When using technology, I will not give my personal email, home address or phone number, or arrange to meet someone that I do not know.
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and always take an adult with me.
- If I see anything I am unhappy with or receive messages I do not like, I will report it immediately.
- When using mobile data on personal devices to connect to the internet during school time, I will act responsibly and in an appropriate manner in accordance with the rules set out in this agreement.
- I will only use apps at school which are age appropriate, this means that I can use 13+ apps when I am in the 3rd form and 16+ when in the Sixth form. This applies even though I may be 13 prior to the start of 3rd form or 16 prior to the start of the Sixth form to ensure parity with my peers whose birthday may fall at the end of the year. I understand that this applies when using school Wi-Fi or when using mobile data.

Use of the College Systems and Facilities

- I will treat all IT rooms and IT equipment with respect and not tamper, change or modify settings to IT equipment.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use internet forums except if it is a discussion room that has been set up by my teacher.
- I will not create or join any Denstone College related social network site/s that is not endorsed

by the school. If I plan to set up a social network site that involves Denstone College or its pupils, I will seek permission first from the Head.

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will not install or attempt to install software of any type on any school device or try to alter computer settings.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

My Behaviour Online

- The messages I send will be respectful, polite and sensible.
- I will not take or distribute photos or videos of members of staff.
- I will not take or distribute photos or videos of pupils without getting their permission first.
- I will only use my mobile phone and other personal devices e.g. smart watches during free time and when I have permission to do so from a member of staff. I will ensure my phone/personal device is turned off during lessons, activities, assemblies, prep etc.
- I understand that if I copy content from the internet or another source and claim the work to be my own this is plagiarism.
- When downloading content from the internet I will ensure this is permitted and not in breach of copyright.
- Any content or work I display on the Internet will be work that I know I would be happy for my family and friends to see.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers at the College. I understand that the College has the right to take action against me if I am involved in incidents or inappropriate behaviour covered in this agreement, when I am out of school and when they involve cyber bullying or the sharing of inappropriate images.

The College may exercise its right by electronic means to monitor the use of the College's computer systems, including the monitoring of websites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the College's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Email

All pupils are given access to a Denstone College email account. Staff may use pupil email addresses for numerous reasons: distribution of prep, providing updates and reminders regarding lessons, communicating House, Boarding, School and Department news, and keeping in contact with pupils during off site study leave or holidays. This provides many communication opportunities and is applicable to pupils of all years.

Pupils can access their Denstone email from any computer in the school and from personal devices linked to the network. Pupils can access emails from Denstone College computers using the desktop shortcut, alternatively if off site or have their personal devices on the college network, emails can be accessed remotely using https://outlook.office.com/

Pupils will be permitted to synchronise their school emails with a personal device. This will facilitate monitoring of emails during the day.

Pupil Responsibilities

- I am expected to check and monitor my school email account once a day (where feasible) during term time and regularly during school holidays.
- I will only use my school email when communicating with members of staff.
- I will be courteous and use correct titles when using school email.
- I will not include any personal information from e-mail addresses such as personal mobile numbers and other email addresses.
- I will not use email in any way that could be harmful or distressing to others. All messages should be polite and responsible. I will report any unpleasant messages sent to me to a member of staff. All email messages are filtered and any inappropriate content is automatically forwarded to the school's IT department. Use of inappropriate language in emails is not acceptable.
- If I receive an email containing an attachment that I am unsure about I must not open it; I will contact IT support to confirm it is safe and does not contain a virus.

I will not:

- Send, access or display offensive messages or images
- Bring in or download any material which contains harmful or inappropriate content.
- Join any mailing lists, chat pages, blogging sites without staff permission
- Respond to any email chain letters
- Share passwords
- Use other pupils' accounts to send email messages
- Create, transmit or forward material that is designed to or would conflict with College business, or undermine the College in any way
- Send large emails e.g. emails with large attachments
- Register with any organisation or website using the school email account unless instructed to do so by my teacher
- Use distribution lists created by the College without prior agreement from a member of staff
- Send personal emails during lesson time without permission from a member of staff

Denstone College promotes the use of email to pupils as a necessity in preparation for moving to University or the workplace.

All pupil activity on the school network and email traffic is monitored by IT Support.

Any breach of these email conditions may lead to withdrawal of the user's access and in some circumstances could lead to further sanctions or even criminal prosecution.

Teams

All pupils are given access to a Denstone College Microsoft 365 account. This gives them access to Microsoft Teams, which can be used for access to lesson resources, class chat and prep.

- I will not share recorded videos/lessons made by teachers outside of the appropriate Team.
- I will not modify or create any video or images of teachers or pupils.
- I will only write appropriate messages in the chat.
- I will only switch on my camera if directed by the teacher.
- If switching my camera on I will ensure I blur or use an appropriate artificial background.
- If switching on my camera I will ensure I am appropriately dressed for a school environment.
- I will only unmute myself when directed to by the teacher.
- I will remain muted during a live lesson and use the hand up feature or the chat to indicate I have a question.
- I will hang up at the end of the lesson once instructed to do so. The teacher must be the last

person in the meeting to hang up.

- I will not re-join a meeting once it has ended.

Denstone College

Pupil Acceptable Use Agreement – The College

Pupil and Parent/Guardian please complete, sign and return to the school office

Pupil: **House:**

Pupil's Agreement
I have read and understand the Pupil Acceptable Use Agreement

I understand that if I fail to comply with this Acceptable Use Agreement, I may be subject to disciplinary action. This may include sanctions such as loss of access to the College ICT systems, detention, suspension, contact with parents and, in the event of illegal activities, involvement of the police.

I understand this agreement will be in place whilst a pupil at Denstone College.

Signed: **Date:**

Parental/Guardian Agreement
I have read, understood and shared with my child the Pupil Acceptable Use Agreement.

Signed: **Date:**

Denstone College

Staff ICT Acceptable Use Agreement

This policy must be read in conjunction with the email, Internet and telephone policy section of the Employment manual. It also needs to be read in conjunction with all IT policies for the school including Data Protection.

All adults working with ICT equipment must ensure that they have read and agree to abide by the following ICT Acceptable User Policy applicable when using Denstone College ICT equipment in your work for Denstone College.

1 General administration

1.1 All staff members have access to the 'I' drive (or 'gendata') for sharing of documentation. This shared area must not be used for storing sensitive documents.

1.2 Each member of staff will have access to a file called My Documents which is held on the 'H' drive. This area is designed for the storing of personal documents and can only be accessed by the individual and the Systems Administrator. It is a useful place to put back up copies of work but this area is limited to 10GB of space.

1.3 All new software requests for installation onto the school network will need to be discussed and approved by the IT Manager and the Compliance Manager. Not all requests will be accepted.

1.4 Staff must ensure that uses of data do not breach the Data Protection Policy (see employment manual).

1.5 Staff use of Denstone College information systems, internet and email may be monitored to ensure compliance with this policy.

2 Using Denstone College IT Systems for personal use:

2.1 Login details and passwords are to remain private and not shared.

2.2 All memory devices such as data sticks must be encrypted. Staff must take their memory stick to the IT support department who will ensure that their memory stick is encrypted prior to use on the network.

2.3 Staff are not permitted to open other people's files without express permission. Attempts to corrupt, interfere with or destroy any other user's information will be seen as a malicious act.

2.4 Staff must not release or share personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or pupil.

2.5 Staff must not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.

2.6 Staff must not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

2.7 Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.

2.8 Staff must log out when their computer session has finished or lock the computer when they are not in attendance.

3 Staff Use of Personal Devices for College Purposes (BYOD)

3.1 Denstone College will provide sufficient IT facilities and equipment for staff where there is a genuine need for this provision. There may be situations however, where staff have a preference for a particular type of equipment they wish to use which may result in the use of personal devices for Denstone College purposes.

3.2 Staff who have decided to use personal equipment will need to be mindful of the data security and online safety issues this brings. Denstone College is responsible for school data that staff possess on personal devices. Staff should always treat personal information with great care and keep it as secure as possible.

3.3 Staff who wish to use a personal device for Denstone College purposes should consult the IT manager. The IT manager may require access to the personal device and may need to install software programs.

3.4 Staff must set secure passwords on personal devices used at Denstone College or for any Destone College business. Passwords must be strong and follow the rules as outlined in section 10 of this policy.

3.5 In a situation where a staff member's personal device has been used for school business and is lost or stolen, the member of staff should change the passwords for all school services accessed from the device and report the incident to the IT Manager as soon as possible.

3.6 When using personal devices for school work, staff should abide by all school ICT policies.

3.7 Any phone calls to pupils or parents must be conducted using either a school handset or if through mobile phones, using the 3CX VOIP software; colleagues are not to disclose their personal phone numbers by calling pupils or parents.

4 Management of Department and Classroom Device Sets

4.1 Teachers are responsible for keeping the devices secure, by means of locked cabinet and classrooms.

4.2 Teachers are responsible for charging the devices.

4.3 Teachers are also responsible for preparing the devices for lessons.

4.4 Teachers are responsible for reporting any issues with the devices to IT Support alongside the device name (which is on a label).

4.5 Booking out of devices will be done through the Room Booking system, this will be done internally within the department.

4.6 Teachers must ensure that pupils log out correctly at the end of each session and the devices are powered off at the end of the day.

4.7 Once a teacher has finished with the devices they should be returned to the trolley and put on charge in preparation for the next use.

4.8 Pupils should not be allowed access to the devices without a member of staff present.

4.9 Teachers are responsible for ensuring the devices stay within the department and are not taken away to be used elsewhere or loaned out / borrowed under any circumstance.

4.10 If teachers wish for additional software to be installed on the devices, they must come through IT Support for this to be centrally managed and tested.

4.11 No food or drink should be used around the devices at anytime.

5 Using Staff E-mail

5.1 It is recognised that email is a widely used mechanism to communicate information to many different groups including staff members, pupils, parents, governors, external organisations and many other individuals and institutions.

5.2 Denstone College wants to ensure a professional image is maintained when communicating to key groups and that the number of potential viruses infiltrating the network as a result of using unsupported email accounts is minimised. The integrity of the use of staff email accounts when communicating internally and externally with reference to Denstone College business during normal working hours, holiday periods or in personal time should be maintained at all times.

5.3 Staff have available a range of options when accessing their email. Staff members have access to MS outlook both as a web version (limited functionality) or desk top version (full functionality). Each system can be used for the purposes of emailing. Staff can also access ISAMs to email staff, pupils and parent/guardian contacts both individually and as groups. Finally, staff can also use smart phones, web mail and other devices to access their Denstone College email account.

5.3.1 Staff should only use their work email accounts when communicating internally and externally with reference to Denstone College related business. All other email accounts e.g. Hotmail, Google mail, Yahoo etc. should not be used for the purposes of communication with pupils, parents, institutions etc.

5.3.2 Staff should protect their privacy and that of others by omitting personal information from e-mail addresses such as personal mobile numbers and email addresses. The approved College email signature is applied automatically.

5.3.3 Staff should aim to respond to parents via email within a 24-hour window of receiving an email. This can be a 'holding' message.

5.3.4 Staff members who are away for extended periods of time should set up an out of office message if away for more than 24 hours.

5.3.5 Staff receive an introduction to their MS Outlook staff email accounts and an introduction to ISAMs. Furthermore detailed staff training information can be found in the following location I:\IT\Training

5.3.6 Any member of staff wishing to communicate with a pupil via email must do so via the pupil's Denstone College email account only. This practice supports the Digital-Safety Policy.

5.3.7 Staff need to remember that anything published electronically may be made public very rapidly and a permanent record is kept of it. Emails are a form of evidence.

5.3.8 Staff need to ensure any use or sharing of data is done so within the guidance of the Data Protection Policy.

5.3.9 Staff need to take care when forwarding an email which includes a string of previously sent emails. Sensitive information may be included in the email trail that should not be shared or communicated with the recipients.

5.3.10 Staff must refrain from showing their Denstone College email account on the classroom smartboards as sensitive information about parents and pupils may be visible to others.

5.3.11 Not all parents and guardians wish to receive electronic based communications. As part of the admissions process and annual data checks, parents are asked if they wish to receive paper mailings. This information is stored in ISAMs in the pupil manager module and can be reported on (see Pupil manager/select all pupils / go to selected pupils/export pupil records/custom fields/ select request paper mailing to run the report). Staff need to be mindful of these families when communicating news electronically and use alternative ways to communicate with the parent such as letter or phone call. The HMO also hold information on these families, this can also be found on ISAMS.

5.4 The IT Support team will not permit or set up the facility to forward Denstone College emails to an alternative email account of choice e.g. Hotmail. Gmail, Yahoo etc.

5.5 To support staff's ability to check and respond to emails, IT Support can set up synchronisation to a range of devices including mobile phones, iPads and other devices. Synchronisation of email will provide staff immediate access to work emails via a device of choice. Details of which devices are supported are available from IT Support.

5.6 Members of staff are able to access their emails remotely when off site. With internet access, all members of staff can access email externally via https://outlook.office.com. Links to staff email and ISAMs are also available from the school website / staff portals.

5.7 Members of staff can use ISAMs as a vehicle to communicate electronically with colleagues, pupils, teaching sets and parents / contacts of pupils both individually and as groups. Information on this process can be found in the following location I:/IT/Training

5.8 In situations where a planned absence from the school is known, an out of office announcement is to be set up providing details of when a return to work is likely. This facility is useful for informing internal members of staff and parents. In addition, contact details for an alternative member of staff to deal with the enquiry should also be provided.

5.9 Staff should regularly practise email hygiene. It is advised that staff keep their inbox to the bare minimum by regularly sorting and deleting emails no longer required. When an email is received containing sensitive information, the sensitive information should be processed or securely saved elsewhere (e.g. saved to a secure area of the i:\ drive, added to CPOMS/iSAMS) and then deleted from email.

6 Using the Internet or e-mail with pupils

6.1 Staff, when using internet or email with pupils, must remind the pupils of what is deemed acceptable use. Staff should provide clear objectives for internet searches, preferably providing good websites rather than simply allowing use of search engines. The School Librarian can also be consulted for valuable online resources. Further details can be found in the Digital-Safety Policy and the Pupil Acceptable Use Agreement.

6.2 In situations where accidental access to inappropriate materials occurs, staff must report the offending site to the Director of IT, IT Manager or IT Technician.

6.3 Staff will encourage pupils to acknowledge the source of information used and to respect copyright.

7 Surveying Staff or Pupils Online

7.1 Staff who wish to gauge opinions using survey programmes such as Survey Monkey, should seek SMT approval through the Head(Internal). A copy of the survey should be sent to the Head in the first instance. This will be considered. It will either be agreed for it to be distributed or not. There may be some edits required before its distribution.

8 Use of Digital Images, Videos and use of Pupil Names

8.1 Permission is requested from parents and parents are informed on pupil entry forms that the school may take and use suitable photographs of their children and use their names for marketing purposes on social media but parents may opt out of either if they wish. Parents are then asked on an annual basis as part of a data check procedure, typically carried out in September, if they wish to continue with this arrangement. Details of parents who have opted out of pupil photo or use of name can be found in ISAMs (See iSAMS / reporting service/run custom report/Pupils not to be used in school media report). Staff need to be mindful of these families when taking digital images and videos or when using pupil names. The Deputy Head Pastoral should be consulted if in doubt.

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

8.2.1 The purpose of the activity should be made clear as to what will happen to the digital images or video.

8.2.2 Digital images and video may be taken by staff or at the direction of staff in any educational activity or school event.

8.2.3 If the taking of pupil images is required, possession of these images must be justified.

8.2.4 Images should not be made during one-to-one situations if at all possible.

8.2.5 All images of children should be stored securely and only accessed by those authorised to do so. Those authorised include teachers, designated safeguarding leads and relevant support staff. An area on Denstone College's network has been created for the storage of digital content. This is found in the following location: I:\Photos.

8.2.6 When taking photos, staff are advised to use general classroom or group activities rather that close up pictures of individual children.

8.2.7 When taking photos of pupil in sporting events all photography should be appropriate.

8.2.8 Where pupil images and videos are to be used for the website and other corporate marketing purposes, content will be approved by the Marketing Department prior to use.

8.2.9 Digital images and video used for social media purposes will be approved by the owner of the social media platform. Digital content used for the Denstone corporate social sites will be approved by the Marketing Department.

8.2.10 You must not take images of pupils using personal devices such as mobile phones or tablets.

8.2.11 Teachers are encouraged to book out a school iPad/device if they wish to do so. These are available from the Marketing department. Most departments have a school issued iPad or smartphone. All images/videos should be removed from the device after use, anything that needs to be kept should be transferred to I:/Photos. All devices should be password protected.

8.2.12 The I:/Photos folder will be managed by the marketing manager who is responsible for securely disposing of imagery in line with the College Records Management and retention policy.

8.3 Children must not be exposed to inappropriate or indecent images. Inappropriate material, such as pornography, must not be brought to work and Denstone College property must not be used to access such material. Pupils are not permitted to have unauthorised access to Denstone 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 person under Denstone College's Safeguarding Policy must be made immediately. Parents are permitted to take photos and videos for their own private use when attending Denstone College events.

9 Group Parental Email and SMS Communication Policy

9.1 Denstone College operates a clear policy for communication with parents and a clear picture of the process, protocols and permission must be understood by all.

9.2 There are several ways to create and manage external bulk/group emails to parents. ISAMs allows for many different combinations of parental groups to be contacted via email. Within ISAMS there are also the options to create and send an email via "Email Wizard" or "Create Email"; the latter is sent using outlook. All bulk/group emails to parents will be sent via the Email wizard method within the ISAMs system.

9.3 Whilst it is possible to email large groups of parents directly it is preferred that to manage the frequency, quantity and quality of communication only the Staff Secretary should send these bulk/group communications. All group communication to parents should go in the Head's weekly newsletter.

9.4 If the communication is more urgent then it is possible to send this out separately and this can be done by the Staff Secretary. Please refer to the emergency communication note below.

9.5 Staff to share their group email communication with the Staff Secretary approximately 5 days in advance or by the Wednesday lunchtime at the absolute latest, if to be included in the Friday newsletter of that week. Staff also need to ensure all details of the message are accurate and any attachments are included. They need to be clear on who the communication applies to.

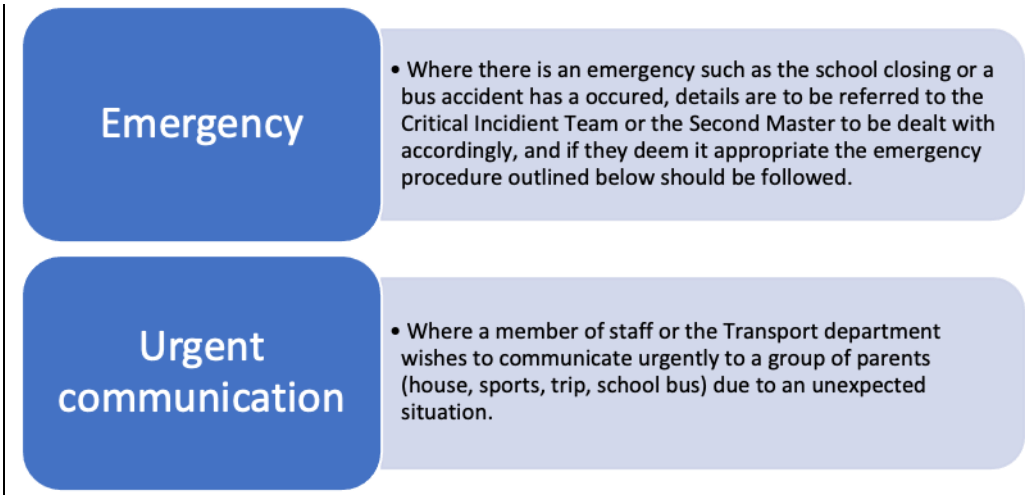
9.6 Staff remain able to email small groups of parents as they do currently on small scale matters and individual parent case concerns. The above email process should only be used when staff wish to communicate in bulk to a wider parental group – in this case the process outlined above should be followed. Staff are permitted to send group parental emails at the tutor group level using MS outlook or ISAMs.

9.7 In addition, Staff should not email groups of pupils with a request for them to forward the email onto their parents/guardians.

9.8 Where parental response/consent is required, an interactive form can be created for the ISAMS parent site or a Trybooking link created or directly through Evolve. Should a member of staff require set up of an interactive form/Trybooking, they need to share details with the Staff Secretary and the SMT Secretary approximately 5 days in advance of when they wish the form to be live.

9.9 Texting Parents via ISAMs

It is expected that text messaging to groups of parents will be limited to emergencies only, or where there is a requirement to communicate issues urgently (such as bussing delays, breakdowns, issues with trips). This is for two reasons: a proliferation of SMS messages dilutes their value, and there are cost implications. The two situations where text messages are permitted are reflected below.



Emergencies

In the case of an emergency, the member of staff approaches a member of the Critical Incident Team (CIT) or the Deputy Head (COP). If it is deemed an emergency together they will send out an emergency text either directly or via Head's Office. If it is not deemed an emergency, the member of staff should use the Urgent process outlined below.

Urgent

When a member of staff needs to communicate urgently with a group of parents he or she should send details to the CIT or Deputy Head (COP) for approval. The Deputy Head (COP) will send the text if it is outside office hours, or may require the Head's Office to send. An urgent text message should not be requested of the Head's Office without the approval of the Deputy Head (COP). The only exception to this is bussing/transport (see below).

Bus/Transport communication

9.10 The transport department will have their own access to the contact information relating to those pupils marked as bus passengers to enable communication regarding bussing issues.

9.11 If however there is an emergency transport situation (to be determined by CIT/ Deputy Head (COP)), then refer to the emergency procedure outlined above which will be managed by the CIT.

10 Passwords

10.1 All passwords used for Denstone College systems must be strong. Strong passwords must contain characters from all of the following categories:

- uppercase letters
- lowercase letters
- base 10 digits (0 through 9)
- non-alphanumeric characters e.g. ~!@#$%^&*+=`|\(){}[]:;'"<>,.?/

currency symbols such as the euro or British pound aren't counted as special characters for this policy setting.

10.2 Passwords must not contain obvious words such as name, department, Denstone or college.

10.3 Passwords should not be the same as any passwords used on any other systems or websites e.g. personal email, websites even if they are sites used for work purposes.

10.4 2 factor or multi factor authentication must be setup where available.

Links to Other School Policies: This policy needs to be read in conjunction with the following policies:

Pupils Acceptable Use Agreement

Data Protection policy

Digital Safety policy

Social Media policy