THE DOWNS
MALVERN

Policy	**Online Safety and Acceptable Use Policy**		
Responsible Member of staff	**Nicholas Vaughan**		
Responsible Governor	**Carey Leonard**		
Approved	**January 2024**	**Next Review Date**	**Jan 2025**
Last Technical Review	**January 2024**		

This policy is relevant to all sections of the school, EYFS, Pre-Prep and Prep, including Boarding.

This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy, Anti-Bullying Policy, Data Protection Policy, Staff Behaviour and Code of Conduct.

Summary Policy Statement

At The Downs Malvern, ICT is an integral part of day-to-day life and has an impact on every child and staff member. We aim for our children to be responsible and effective users of technology and they are provided with opportunities to use ICT in their academic and extra-curricular life at School. We have robust systems in place to keep our children safe whilst using technology as a teaching and learning tool. Beyond this, all members of the School Community are educated in avoiding the potential dangers associated with online lives outside of the School.

Contents

Statement of General Policy 3
Roles and Responsibilities 3
Communicating School Policy 5
Making Use of ICT and the Internet in School 5
Learning to Evaluate Internet Content 6
Managing Information Systems 6
Email Protocol 7
Published Content and the School Website 9
Using Photographs of Individual Children 9
Complaints of Misuse of Photographs or Video 10
Training 10
Social Networking, Social Media and Personal Publishing 10
Mobile Phones and Personal Devices, including Smart Watches 12
Cyberbullying 14
Safe Use of ICT 16
Managing Emerging Technologies 16
Breaches of Policy 17
Acceptable Use of ICT in School 17
Appendix 1: Key Stage 3 and Personal Device ICT Acceptable Use Agreement 19
Appendix 2: Key Stage 2 ICT Acceptable Use Agreement 21
Appendix 3: Key Stage 1 ICT Acceptable Use Agreement 23

Statement of General Policy

The Downs Malvern recognises that ICT and the Internet are integral tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to collaborate and share ideas can benefit all members of the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it responsibly, appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. (See section: Cyberbullying. Also, see Anti-Bullying Policy

Roles and Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety also falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- ensure an online safety policy is in place, reviewed every year and is available to all stakeholders;
- ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive;
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to; and
- hold the Headmaster and staff accountable for online safety.

Headmaster and SLT

The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-Ordinator. Any complaint about staff misuse must be referred to the Deputy Head (Pastoral) at the School or, in the case of a serious complaint, to the Headmaster, to ensure:

- access to induction and training in online safety practices for all users;
- appropriate action is taken in all cases of misuse;
- Internet filtering methods are appropriate, effective and reasonable;
- staff or external providers who operate monitoring procedures be supervised by a named member of SLT;
- pupil or staff personal data as recorded within school management system sent over the Internet is secured;

- the School works in partnership with the DfE and the Internet Service Provider and school ICT Manager, Steve Cragg, to ensure systems to protect students are reviewed and improved;
- the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly; and
- the Senior Leadership Team will receive monitoring reports from the Online Safety Co-Ordinator.

Online Safety Co-Ordinator

The Online Safety Co-ordinator will:

- Lead E-safety meetings;
- Work in partnership with the DFE and school ICT Manager to ensure systems to protect students are reviewed and improved;
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly;
- Receive reports of E-safety incidents and create a log of incidents to inform future online safety developments;
- Report to the Senior Leadership Team; and
- Liaise with the nominated member of the governing body & Headmaster to provide an annual report on online safety.

Network Manager / Technical Staff

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply;
- That users may only access the networks and devices through a properly enforced password protection policy;
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person;
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headmaster; online safety coordinator for investigation / action / sanction;
- That monitoring software / systems are implemented and updated as agreed in school policies.

Staff

- Staff are responsible for the security of their terminal and must not allow the terminal to be used by an unauthorised person.
- Staff should keep their personal password confidential and change it regularly.
- When leaving their terminal unattended, staff should ensure they log off the system to prevent unauthorised users using the terminal in their absence.
- Use of the internet and email system is for legitimate school business only. Searching for, or viewing, or downloading web pages, the content of which is offensive, obscene, or discriminatory will constitute gross misconduct. Staff must adhere to the use of Social Media, email and internet use laid out in this policy.

Communicating School Policy

This policy is available for staff online on the school's website. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHCE lessons where personal safety, responsibility, and/or development are being discussed.

Making Use of ICT and the Internet in School

The Internet is used in school to raise educational standards, aware of the online/digital environment to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need to enable them to progress confidently and safely into a professional working environment when they leave school. Some of the benefits of using ICT and the Internet in schools are:

For Pupils:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries;
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world;
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet;
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen;
- Access to learning whenever and wherever convenient;
- Freedom to be creative;
- Freedom to explore the world and its cultures from within a classroom;
- Social inclusion, in class and online;
- Access to case studies, videos and interactive media to enhance understanding;
- Individualised access to learning; and
- The use of the Microsoft 365 suite.

For Staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management via iSAMS
- Use of Teams for online teaching, access to departmental files and staff files.

For Parents:

- Communication between School and Home on issues related to the education of their children and issues faced by the challenges and potential dangers of the online world.
- The main forms of communication are via Email, using iSAMS. Staff may contact a parent directly through Outlook for low-level housekeeping, but any correspondence of which a permanent record is required should be sent through the iSAMS email wizard. Staff should not contact multiple sets of parents through Outlook, to prevent infringing GDPR. See Email protocol, page 7 for further detail.

Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- Use age-appropriate tools to search for information online; and
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils.

Pupils' keystrokes are monitored when logged into their school accounts, using Impero; SLT and IT staff are alerted to violations.

If a member of staff or pupils discover unsuitable sites then the URL will be reported to ICT services at Malvern College.

Any material found by members of the school community that is believed to be unlawful will be reported to the online safety coordinator and the SLT.

Regular software and broadband checks will take place to ensure that filtering services are working effectively, including, but not restricted to, the requirements of Prevent Duty.

Managing Information Systems

The Downs Malvern is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The Network Manager will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off-site is encrypted and in accordance with our Data Protection Policy.
- Making sure that unapproved software is not downloaded to any school computers.
- Files held on the school network will be regularly checked for viruses.
- The use of user logins and passwords to access the school network will be enforced.
- Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.
- Compliant with existing Data Protection legislative requirements.
- Filters imposed by Malvern College ICT services screen all internet traffic and block sites which are deemed to be inappropriate. Internet searches are filtered for profanities, spam and any inappropriate content, including those that would fall under Prevent Duty to keep children safe from extremist material.
- Impero Software Actively monitors website titles, content, open applications and typed words for safeguarding, security and behavioural misuse of the computers – taking screenshots and (optionally) blocking access as Network Manager sees fit.
- Virus protection throughout the school is updated daily.

- Malvern College ICT services provide staff with regular data protection training and CPD. Regular ‘fake’ spam emails are sent to staff members to ensure that they do not click on unverified links. Staff who fail the test get enlisted to complete further online data protection CPD.

For more information on data protection in school please refer to our **Data Protection Policy** found in thedownsmalvern.org.uk/about-the-downs/policies.html.

Email Protocol

The School uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to. See Staff Behaviours Policy and Staff Handbook.

Microsoft Teams is also used for messages between staff and pupils. The same usage rules apply as for emails

Legal Action Against the School

Messages sent over the email system can give rise to legal action against the School. Claims for defamation, breach of confidentiality or contract could arise from a misuse of the system. It is therefore vital for email messages to be treated like any other form of correspondence and where necessary hard copies should be retained. Messages are disclosable in any legal action commenced against the School relevant to the issues set out in the email.

The School’s Rights

The School reserves the right to retrieve the contents of all incoming and outgoing messages for the purpose of monitoring whether the use of the email system is legitimate, when employees are off sick or on holiday, to find lost messages or to retrieve messages lost by computer failure, to assist in the investigations of wrongful acts or to comply with any legal obligation.

The School reserves the right to monitor email messages sent and/or received and to monitor usage of the Internet.

General Rules

Should staff receive an email message which has been wrongly delivered to their email address, they should notify the sender of the message by redirecting the message to that person but NOT in the case of SPAM which should be deleted immediately. Further in the event the email message contains confidential information, staff must not disclose or use that confidential information. Should staff receive an email which contravenes this policy the email should be brought to the attention of the SLT.

Misuse of the email system in breach of these rules will be treated as misconduct.

Misuse of the email system by transmission of any material in any of the following categories will constitute gross misconduct:

- defamatory;

- offensive or obscene;
- untrue or malicious;
- discriminatory on grounds of race, sex, marital status, disability, sexual orientation,
- religion or religious belief & philosophical beliefs or age;
- the School's Confidential Information (as defined the contract of employment); and
- protected copyright material.

School Email Accounts and Appropriate Use

- All Prep School children have their own Microsoft 365 account. Children should not access any other email accounts in school.
- Pre-Prep students do not have access to email accounts, as they do not have individual school accounts.
- Children do not have access to external web-based email accounts such as Hotmail, Google mail etc, unless supervised in the Boarding House.
- Pupils must complete, sign and understand the Pupil Usage Acceptance Agreement before using the School's ICT.
- Staff have a school Microsoft 365 email account which is accessible via the school network, remote access or via Smartphone (iPhone or Android). Staff are allowed to access their own personal emails via the school network, though this should not be done during school hours.

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers for school related matters. Emails should be sent using iSAMS for multiple parent recipients, so that addresses are confidential and messages recorded. Personal email accounts should not be used to contact any of these people.
- Staff are representing the school at all times and should take this into account when entering into any email communication. Emails sent from school accounts should be professionally and carefully written, in accordance with the professional standards of any other form of written communication. The content and language used in the message must be consistent with best School practice. Messages should be concise and directed to those individuals with a need to know. Emails to parents from iSAMS should have clearance from a member of SLT for proofreading and double-checking.
- The blind carbon copy facility (BCC) should always be used to protect customer/client confidentiality, on occasions when iSAMS cannot be used for emailing groups of parents.
- Confidential information should not be sent externally and in some cases internally, by email without express authority and unless the messages can be lawfully encrypted.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Pupils should be aware of the following when using email in school

Pupils will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use school-approved email accounts;
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves; and
- Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online.
  Pupils will be educated through the Computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Published Content and the School Website

The Downs Malvern website is viewed as a tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published (unless with express consent), and details for contacting the school will be for the school office only. For information on the school policy on use of children's photographs on the school website please refer to **our** Data Protection Policy**.**

As a marketing tool, the school website is maintained by the Marketing team and third-party website specialists as they see fit.

Using Photographs of Individual Children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. The school is careful to make sure that images published on the school website and social media platforms are difficult to reuse or manipulate through browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the parent's and school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child, unless express parental consent have been obtained. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of pupils such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

For more information on safeguarding in school please refer to our school Safeguarding and Child Protection Policy.

Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our Complaints Policy and Procedure for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools Safeguarding and Child Protection Policy.

Cyberbullying and sexting by pupils will be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm and will be managed through our anti-bullying procedures (See our Anti-Bullying Policy) and Safeguarding and Child Protection Policy. Serious incidents may be managed in line with Safeguarding and Child Protection Policy.

Training

Pupils

Many pupils own or have access to handheld devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community. See Guidance for Pupils on the Acceptable use of ICT in School and Cyberbullying.

Parents

The Parent Zone on the school website provides parents with advice and information about online safety. See also Section 18: Guidance for Parents on the Acceptable Use of ICT in School. Face-to-face sessions with parents focus on strategies to extend online safeguarding beyond the School and into the family home.

Teaching Staff

All teaching staff receive online safety training on an annual basis. In addition, INSET sessions related to the latest online safety trends are held at different times of the year.

Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school as the majority of our pupils do not meet the minimum required age. There are various restrictions on the use of these sites in school that apply to staff.

All network users must use an appropriate password and always remember to log out after use. It is the responsibility of the user and it is critical that staff do not allow children access to their own personal account.

This policy recognises that social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHCEe about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways when they meet the required minimum age limit. They are all made fully aware of the school’s code of conduct regarding the use of ICT and technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

Staff Use of Social Media

- Staff should be professional, responsible and respectful when using social media.

- When using social media staff must be conscious at all times of the need to keep their personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their work for the School and their personal interests.

Staff must not:

- engage in activities involving social media which could damage the reputation of the School, even indirectly.
- represent their personal views as those of the School on any social media. Staff should write in the first person and use a personal email address.
- discuss personal information about School pupils, staff members and other professionals they interact with as part of their job at the School on social media.
- include the School’s logos or other trademarks in any social media posting or in their profile on any social media.
- use social media and the Internet in any way to harass, bully, unlawfully discriminate against, attack, insult, abuse, disparage or defame pupils, their family members, staff members, other professionals, other organisations or the School as an institution; to make false or misleading statements; or to impersonate colleagues or third parties.
- express opinions on behalf of the School via social media, unless expressly authorised to do so by the Marketing Department and SLT. Staff may be required to undergo training in order to get such authorisation
- edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer’s IP address and the intervention will, therefore, appear as if it comes from the School.
- identify themselves as employees of the School or service providers for the School in their personal web space (use of professional web space such as LinkedIn is up to the user’s discretion, keeping in mind that anyone such as parents, students and colleagues can access profiles and staff must always comply with this policy). This is to prevent information on these sites being linked with the School and to safeguard the privacy of staff members, particularly those involved in providing sensitive front-line services.
- accept ‘friend requests’ from current pupils or recent leavers they receive in their personal social media accounts.
- “check in” or tag their photos/videos at the School (this includes but is not limited to Facebook, Instagram, Twitter, Pinterest).
- use School email addresses and other official contact details for setting up personal social media accounts or to communicate through such media. The use of School email addresses to create or join a School sanctioned social media site is appropriate.
- on leaving the service of the School, contact the School’s current pupils by means of personal social media sites. Similarly, staff members must not contact current pupils from their former schools by means of personal social media unless they are family-

related/close friends with parents. It is advised to maintain professional conduct while communicating with former students for work or personal reasons.
  - have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
  - have contact through any personal social media with any current pupils, whether from the School or any other school, unless it is for professional contact or the pupils are family members.

- Staff must be:
  - respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the Internet for anyone to see.
  - accurate, fair and transparent when creating or altering online sources of information on behalf of the School.

Furthermore:

- If staff are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until they have discussed it with their Department Head.
- If staff see social media content that disparages or reflects poorly on the School, they should contact a member of Senior Leadership Team (SLT).
- The School permits limited personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the Internet or social media should not be used during contact time (for teachers and teacher assistants), should never involve unprofessional or inappropriate content and must always comply with this policy.
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and opt out of public listings on social networking sites to protect their own privacy.
- Staff members can only use officially sanctioned School social media tools for communication on behalf of the School. Requests for this type of communication should go via the Marketing Department who have access to the relevant social media tools.
- There must be a strong pedagogical or business reason for creating official School social network sites to communicate with pupils or others. Staff members must not create sites for trivial reasons which could expose the School to unwelcome publicity or the posting of unwelcome material or damage its reputation.
- Official school sites must be created according to the requirements provided by the Marketing Department. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.
- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites. We are responsible for the safeguarding and protection of children.

Mobile Phones and Personal Devices, including Smart Watches

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make users more vulnerable to cyber bullying;
- Can be used to access inappropriate internet material;
- Can be a distraction to learning;
- Are valuable items that could be stolen, damaged, or lost; and
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

Cameras, iPads, personal devices and mobile phones are prohibited in the toilets or changing areas.

Pupils Mobile Phones

The Downs Malvern has a no mobile phone policy for pupils during day school. Under very exceptional circumstances, parents can seek permission from the Headmaster for a day pupil to have his or her mobile phone on the premises; in this case, the mobile phone should be handed into the school office immediately upon arrival and the pupil must ask a member of staff to return it at the end of the day. The phone is not to be taken into day school. Boarders are allowed access to their mobile phones for a limited time each evening to contact family members (see Boarding Policy).

Smart watches are those with internet connectivity. More recent versions are able to make telephone calls without the presence of a mobile phone. Such devices are not permitted in school. In essence, any watch that is 3G, 4G or 5G or Wi-Fi enabled is not permitted around the school. Any such watch will be removed and stored until it can be returned to the parent at the end of the school day.

Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy.

Visitor's Mobile Phones

Visitors and parents should follow the criteria set out in Guidance of Parents on the Acceptable Use of ICT in School. Please also see Data Protection Policy.

Staff personal devices or mobile phones

The school expects staff to lead by example. When on-site, personal mobile phones should be on 'silent' (or switched off) and stored out-of-sight of pupils.

Staff need their mobile phone for two-factor authentication to access CPOMS. When required, this should be done out-of-sight of pupils.

Some staff members receive school emails on their phone (this is a necessity for certain staff members, for example, Games teachers or those on trips). This should be done discreetly.

Staff off-site (for example, on fixtures or trips) may need to be phoned by the school, or by other accompanying staff members, as a matter of urgency or for logistical reasons. Those staff are not required to have their phones on silent.

There are times when staff members may need to make a personal call, email or text (for example, for a medical appointment). This should be done outside lesson time and out-of-sight and hearing of pupils (for example, in the staffroom or an office).

Only under exceptional circumstances, should staff use their own phone to contact parents. If Staff are involved i activities where they may find themselves in this position they should ensure that their own devices are equipped with the 3CX App.

Staff are not permitted to take photos or videos of pupils on their personal devices. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment (for example, iPads) will be used for this.

Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in **Safeguarding and Child Protection Policy**, or in the staff contract of employment.

iPads and School Laptops

- Staff should make sure that iPads and school laptops are returned to the trolley, and all accounted for at the end of the lesson. The iPads and laptops should be locked away at the end of the day and a check made that all are accounted for.
- iPads do not require an individual pupil account to be used. The Head of ICT and Safeguarding Deputy will regularly conduct random searches of school iPad and contents, checking that content is appropriate and in accordance with responsible use guidance. In addition, daily reports are provided via Impero detailing suspicious search queries.
- Guidance is provided for students and staff in our Acceptable Use Policies.

Cyberbullying

The Downs Malvern embraces the advantages of modern technology in terms of the educational benefits it brings, however the School is mindful of the potential for bullying to occur. Central to the School's Anti-Bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'. The School also recognises that it must 'take note of bullying perpetrated outside School that spills over into the School'. Under powers granted by the EIA 2006, the Head is able to police cyberbullying, or any bullying aspects carried out by pupils even at home. Further information about specific strategies or programmes in place to prevent and tackle bullying is set out in the Anti-Bullying Policy and Safeguarding and Child Protection Policy.

Definition of Cyberbullying

Cyberbullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself. By cyberbullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones.
- The use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites.
- Using email to message others
- Hijacking/cloning email accounts
- Making threatening, abusive, defamatory, or humiliating remarks in chat rooms, to include Facebook, YouTube and Ratemyteacher

Legal Issues

Cyberbullying is generally criminal in character. The law applies to cyberspace.

- It is unlawful to disseminate defamatory information in any media including internet sites.
- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

The Downs Malvern educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through PSHCEe and in ICT lessons and assemblies, continue to inform and educate its pupils in these fast-changing areas.

The Downs Malvern trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. The Downs Malvern endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present. Where appropriate and responsible, The Downs Malvern audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, The Downs Malvern reserves the right to take action against those who take part in cyberbullying.

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.
- The Downs Malvern supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.
- The Downs Malvern will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.
- The Downs Malvern will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the Headmaster any example of cyber-bullying or harassment that they know about or suspect.

Guidance For Staff
If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image.
- Go with the pupil and see the Headmaster, or in his absence, a member of the Senior Leadership Team.

Computers

- Ask the pupil to get up on-screen the material in question.
- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Accompany the pupil, taking the offending material, to see the Headmaster.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Guidance For Pupils
If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your Form Tutor, a member of staff or the Headmaster.

- Do not answer abusive messages but log and report them
- Do not delete anything until it has been shown to your Form Tutor, a member of staff, parents/guardian or the Head (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyberbullying)
- Do not give out personal IT details
- Never reply to abusive emails
- Never reply to someone you do not know
- Stay in public areas in chat rooms

Guidance For Parents
It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. The Downs Malvern informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying.

- Parents can help by making sure their child understands the School's policy and, above all, how seriously The Downs Malvern takes incidents of cyberbullying
- Parents should also explain to their sons or daughters the legal issues relating to cyber-bullying
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything
- Parents should contact the Headmaster as soon as possible. A meeting can then be arranged with the Headmaster, which may involve other relevant members of staff
- If the incident occurs during the holidays, The Downs Malvern reserves the right to take action against bullying perpetrated outside the school that spills over into the school.

Safe Use of ICT

Instructions for the safe use of ICT are explained and discussed with pupils in assemblies, PSHCEe classes and ICT classes. Advice is displayed in the ICT suite.

E-Safety at Home
Several websites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Further support and guidance may be obtained from the following:

www.familylives.org.uk
www.nspcc.org.uk
www.nationalbullyinghelpine.co.uk

Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess and conduct a Data Impact Assessment, where necessary (and in accordance with the Data Protection Policy) any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting Personal Data
The Downs Malvern believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and

individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. See Data Protection Policy.

For further information on how we look after your personal data, please refer to our Privacy Policy online and our Data Protection Policy.

Remote Access Policy
Staff are able to access the school iSAMS network and Malvern College Microsoft 365 network at home via Remote Desktop Protocol (RDP). All users:

- Are able to access a remote desktop session.
- Are able to access the same files and resources as they can when logged onto a school computer on-site.
- Are asked to be vigilant and to log off after use.

Reporting on Compliance and Effectiveness
An annual report, covering compliance with and summaries of:

- The daily reports received (at 7am) by the Head of ICT, showing the previous day's activity with children using the computers, so that any issues can be quickly investigated; examples include:
- Any suspicious search queries using Google.
- The length of time each child spent using the Internet.
- Any suspicious words typed on a computer by a child.

Breaches of Policy

Any breach of this Policy may lead to disciplinary action being taken against the staff member/s involved up to and including dismissal, in line with the School's Disciplinary Policy and Procedures. Any staff member/s suspected of committing a breach of this policy will be required to cooperate with the School's investigation, which may involve handing over relevant passwords and login details.

Staff member/s may be required to remove any social media content that the School considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Any non-compliance will be taken seriously, logged and investigated appropriately in line with our disciplinary policy.

Acceptable Use of ICT in School

Guidance for Parents on the Acceptable Use of ICT in School
The Downs Malvern acknowledges that technology is an integral part of 21st century life and parents wish to use latest developments to support and record their children's time at school. However, in the interests of safety, security and privacy we would ask that parents follow the following guidance on the use of mobile telephones, tablets and all other personal technological devices.

Making Telephone Calls or Using Mobile Devices

- Parents / carers are respectfully advised that they should not make telephone calls or use any mobile devices in classrooms or communal areas.
- Parents/ carers should not attempt to contact their child during the school day on the child's mobile phone or device.
- Parents / carers should not contact members of staff using the teachers' personal mobile phones.

- Parents/carers are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact.

Digital Images (still photographs and videos)

- Parents are allowed to take photos and videos of their own children during school events, performances and assemblies
- To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites or other public areas of the internet.
- If parents would prefer their child/children did not feature in school photographs or on social media platforms linked to the school they should let the school know in writing.
- Parents are also requested not to post images of members of staff on social media platforms.

Parental Awareness

- The school will endeavour to assist parents with their awareness of developing technologies and give advice on how to support children towards safe, responsible and appropriate use of the internet, social media and developing technologies. This may be covered through newsletters, talks or a range of other activities.
- It is recommended that parents and children develop their own Online Agreement for use at home that is respected and followed by all members of the family.

Guidance For Pupils on the Acceptable Use of ICT in School

At The Downs Malvern, within PSHCEe and ICT lessons and assemblies, children are provided with a comprehensive e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. At the beginning of each school year, Children are required to read, understand, and sign the appropriate age-related ICT Acceptable Use Agreements on the following pages.

Appendix 1: Key Stage 3 and Personal Device ICT Acceptable Use Agreement

Dear Parents and Guardians,

The pupils have been talked through the following points on how to use ICT equipment safely and responsibly in school. It would be greatly appreciated if you could go through this agreement with your child again at home, sign it, and have it returned to their Form Tutor.

Many thanks.

KEY STAGE 3 AND PERSONAL DEVICE ICT ACCEPTABLE USE AGREEMENT

Pupil's Name:_________________________________ **Form:** ________

If used correctly, being able to bring your device into school has the potential to hugely enhance your learning experience at The Downs Malvern. The following rules will keep everyone safe and ensure that all pupils have a positive experience when accessing their device and the internet.

Using the School's Wifi & Cloud Systems:

1. I understand that my device is only to be used for educational purposes.
2. I will only use my device when instructed to do so by a teacher.
3. I understand that my computer should only be used in a classroom.
4. I must only access the School's Wifi (Downs Malvern Wifi) and Cloud systems with the login and password I have been set up with.
5. I must not access other pupils' files, directories or Emails;
6. I must not bring into School any external media such as USB memory sticks.
7. I must remember to acknowledge copyrighted material where appropriate.
8. I must respect the School's ICT system security at all times.

Using the Internet to Browse Web Pages:

1. If using a device during prep, I will ask permission from the supervising member of staff before I access the web pages. I will inform them of the websites that I will be visiting and access only these websites throughout the prep session.
2. I know that what I type on the computers and iPads, and what I access on the internet is being constantly monitored by the school. I understand the reasons for the school doing this.

3. I will inform a teacher if I encounter any threatening, unpleasant or inappropriate material. I understand that by doing this I am helping to protect myself and other pupils.

Using the Internet for Communication:

1. I must understand that all communications sent to or received from my account are monitored by the School's ICT systems and may be read by members of staff.
2. I understand and will remember that the use of social media platforms, such as Facebook, Instagram, Twitter, Snapchat, TikTok, Whatsapp, Discord etc, are not allowed.
3. I will only send respectful, polite, and responsible messages.
4. I will only send electronic messages to people I know, or to people my teachers have approved.
5. I will only use my school email address or school Teams account when communicating with staff or peers. I will not use my personal email addresses in school.
6. I will not reveal any personal information when sending electronic messages or share any personal information or photographs of myself or others.
7. I will inform a teacher if I receive any unpleasant messages (e.g via Teams Chat). I understand that by doing this I am helping to protect myself and other pupils.
8. I will not view / share / listen to inappropriate words, images, music or videos.
9. I will never use electronic communication to arrange to meet people outside of school hours and I will inform a teacher immediately if I am contacted by a stranger.
10. During the school day, I will never contact family members, or friends who do not belong to the school, on my device.
11. I will only take photographs for educational purposes, and I will gain the permission of a teacher before I do so.

Protecting my device in school:

- I will always carry my device around school in a protective case.
- I will take my device to my form room's secure location at break and lunch time.

I agree that, if I cannot follow these expectations, my device will be removed and returned home until further notice.

Pupil's Signature: ____________________

Parent's Signature: _________________________

Date _______________

Appendix 2: Key Stage 2 ICT Acceptable Use Agreement

Dear Parents and Guardians,

The pupils have been talked through the following points on how to use ICT equipment safely and responsibly in school. It would be greatly appreciated if you could go through this agreement with your child again at home, sign it, and have it returned to their Form Tutor.

Many thanks.

<u>KEY STAGE 2 ICT ACCEPTABLE USE AGREEMENT</u>

Please tick the boxes to show you agree.

1. I will only use a device at school when there is a teacher present in the room. □

2. I will respect the school's ICT resources and do nothing to disable or cause any damage to them. □

3. I will ask permission before entering any website, or downloading programmes, apps or files from the Internet, unless my teacher has already approved the site. □

4. I will get permission from the owner before I look at, modify or delete anyone else's files. □

5. Any electronic communication I send, from any sort of device, will be polite and responsible. If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately. □

6. When in school, I will only use my school email address. □

7. I will choose a secure password and keep it private. □

8. I will ask my teacher's permission before using any personal electronic devices or bringing files into school. □

9. I will only use Microsoft Teams for educational purposes.	

10. I will always behave in a responsible manner when using devices both in and out of school and not do anything that goes against the school's Code of Conduct. I understand that I must follow these rules if I am to be allowed to use computer equipment.	

11. If using a device during prep, I will ask permission from the supervising member of staff before I access web pages. I will inform them of the websites that I will be visiting and access only these websites throughout the prep session.	

11. I know that what I type on the computers and iPads, and what I access on the internet is being constantly monitored by the school: I understand the reasons for the school doing this.	

I understand that I must follow these rules if I am to be allowed to use computer equipment.

Pupil's Name: ______________________________________ Class: _________

Date: _____________

Parent's Signature: ___________________________

Appendix 3: Key Stage 1 ICT Acceptable Use Agreement

Dear Parents and Guardians,

The pupils have been talked through the following points on how to use ICT equipment safely and responsibly in school. It would be greatly appreciated if you could go through this agreement with your child again at home, sign it, and have it returned to their Form Tutor.

Many thanks.

KEY STAGE 1 ICT ACCEPTABLE USE AGREEMENT

Please tick the boxes to show you agree.

1. I will only use ICT equipment if there is an adult in the room. □

2. I will look after ICT equipment properly and use it carefully. I will never leave an iPad on the floor. □

3. I will only use technology for the reason I have been asked to use it. □

4. When using Seesaw, if I ever make a comment on a classmate's work, I will always be kind and respectful. □

5. I will only look at, change, or delete my own files. □

6. I will ask the teacher before I print anything. □

7. If I see anything that makes me unhappy, I will tell my teacher. □

Pupil's Name: ______________________________________ Class: _________

Date: _____________

Parent's signature: ____________________________