Devonshire House Preparatory School

E-Safety Policy

Last review date	*October 2025*
Next review date	*July 2026*
Lead reviewer	*David Zerafa*

Serving North London Families

Devonshire House is a co-educational prep school, offering unparalleled preparation for senior school and life thereafter. Our unwavering emphasis on individual growth, within an inclusive community, balances traditional values and modern practice to inspire fearless life-long learning.

Our school values are:

- **Growth** – we reach high
- **Courage** – we learn fearlessly
- **Wonder** – we are inspired to find our spark
- **Belonging** – we care and come together

This policy is available on the Policies page of the School SharePoint and policies page of the School website and can be made available in large print or other accessible format if required; such requests can be made by email to: arkwright@dhprep.co.uk

Development / Monitoring / Review of this Policy

This e-Safety Policy has been developed by SLT and originally rolled out to all staff and pupils in Sept 2023. It has been amended in 2025 to reflect the ongoing changes in school IT and E-Safety.

Schedule for Development / Monitoring / Review of this Policy

This e-Safety policy will be reviewed annually by the Governance:	Annually, usually at the June meeting
The implementation of this e-Safety policy will be monitored by:	The Digital Learning team, The DSL and the Head

Monitoring will take place at regular intervals:	Termly – a standing item on the SLT and Governance agenda
Governance will receive a report on the implementation of the e-Safety policy generated by the Head (which will include anonymous details of e-Safety incidents) at regular intervals:	Annually
The e-Safety Policy will be reviewed annually, or more regularly, in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	June 2026
Should serious e-Safety incidents take place, the Head will be informed. They will determine what action to be taken. If the issue involves safeguarding concerns, then the Safeguarding and Child Protection Policy will be followed to determine whether to inform external persons / agencies.	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity

Key People

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Louise Reen
Deputy Designated Safeguarding Leads / DSL Team Members	Jude Swailes (DDSL), Danica Belzer (DDSL)
Governor for safeguarding	David Goodhew
Curriculum leads with relevance to online safeguarding and their role	David Zerafa – Head of Technology & Digital Lead Jude Swailes – Head of PSHEE (Middle + Upper School) Lucy Peacock - PSHEE Lead (Lower School)
The IT Support Function	The IT Support Function is currently made up of the school Digital lead (David Zerafa), the Regional Head of IT (Kevin

	Chung) and the Managed Service Provider

Aims

This policy aims to promote a whole school approach to online safety by:

1. Setting out expectations for all Devonshire House School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
2. Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
3. Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
4. Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
5. Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

6. Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope of the Policy

This policy applies to all members of the Devonshire House School community (including staff, governors, volunteers, contractors, pupils, parents/carers, visitors) who have access to and are users of our digital technology networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

The School will deal with e-Safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, such as the Safeguarding and Child Protection, Behaviour and Discipline, Anti-bullying Policies. It will, where known and appropriate, inform parents of incidents of inappropriate e- Safety behaviour that take place out of school.

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

All Staff:

are responsible for ensuring that:

- They have an up-to-date awareness of e-Safety matters and of the current e-Safety Policy and practices.
- They have read, understood and agreed to the Staff AUP agreement, in conjunction with this policy, the main safeguarding policy, the code of conduct and relevant parts of KCSIE to support a whole-school safeguarding approach.
- This includes reporting any concerns, no matter how small, to the designated safeguarding lead, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.
- Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.
- All digital communications with other staff, pupils and parents/carers are on a professional level.
- They help pupils understand and follow the e-Safety and acceptable use policies.
- They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Head and Senior Leadership Team

The Head has a duty of care for ensuring the safety (including e-Safety) of members of the school community, Key Responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding

- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data- protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead and Deputy DSLs

Key Responsibilities

The DSL should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

- Ensure an effective whole school approach to online safety as per KCSIE

- Working to ensure filtering and monitoring systems are robust.

- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused

- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns

- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.

- Remind staff of safeguarding considerations as part of a review of remote

learning procedures and technology, including that the same principles of online- safety and behaviour apply

- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).

- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."

- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends.

- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.

Governance

Key Responsibilities:

- Approval of the e-Safety Policy and for reviewing the effectiveness of the policy. Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Receipt of the termly e-Safety report from the Head
- Regular monitoring of e-Safety incident logs
- Regular monitoring of changes to filtering

E-Safety Management:

The school ICT committee comprises the head of IT (Technology), the regional head of IT (Dukes), the Managed Service Provider, the school DSL and SLT. The committee:

- Take day-to-day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school e-Safety policies and documents.
- Email staff at the start of each year to remind them of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Arrange for the provision of training and advice for staff , parents and Governance (in liaison with the Head of PSHEE).
- Are responsible for e-Safety education for pupils.
- Receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments
- details are in the section 'Responding to Incidents of Misuse' section of this policy.

- As a representative of this group the Head will meet with Governance to discuss current issues, review incident logs and changes to filtering – see 4.1 above.
- Report regularly to the Health and Safety Committee.
- Deal with incidents.
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

The Managed Service Provider, IT Infrastructure and Support

is responsible for ensuring the following:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the School meets all e-Safety technical requirements as laid out in the Internet Security Information document.

- That users may only access the school's networks and devices if properly authenticated and authorised.
- Collaborating regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards,
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- The filtering policy is applied and updated on a regular basis.
- That they keep up-to-date with e-Safety technical information in order to carry out their e-Safety role effectively and to inform and update others as relevant.
- That the use of the school's networks and devices is regularly monitored to ensure compliance with the Acceptable Use Policies (AUP'S) in order that any misuse or attempted misuse can be identified and reported to the DSL for investigation.
- That monitoring software and systems are kept up to date.

School digital lead

- When able, helps the Managed Service Provider with all manors onsite IT support issues
- Works with the Managed Service Provider and school leadership to sure all pupil devices and
- pupil login details and safe, secure and updated each academic year
- Identifies and provides where appropriate additional training to staff, parents and pupils
- Works withs with all parties to make sure the School meets all e-Safety technical requirements as laid out in the Internet Security Information document.
- That users may only access the school's networks and devices if properly authenticated and authorised.
- Collaborating regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support Managed service provider, DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology,
- Helps DSL and leadership team maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy

- That they keep up-to-date with e-Safety technical information in order to carry out their e-Safety role effectively and to inform and update others as relevant.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil AUP Agreements for Devonshire House School.
- Key Responsibilities:
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions.

Parents

Play a crucial role in ensuring that their children understand the need to use the Internet / Mobile devices in an appropriate way.

Parents are asked to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of: Digital and video images taken at school events:

- Access to any Parent Portals
- Their children's personal devices in the school.

Community Users

Overall, we do not allow access to the school network by outside visitors however, those who do access school systems as part of the wider school provision will be expected to sign a Visitors' AUP agreement before being provided with access to school systems.

Policy Statements

Education – Pupils

E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, and will be provided in the following ways:

- An e-Safety curriculum is provided as part of Technology, PSHEE and other lessons and is regularly revisited
- Key e-Safety messages are reinforced as part of a planned programme of assemblies

- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils are helped to understand the need for the Pupil AUP agreement and encouraged to adopt safe and responsible use both within and outside school
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT Support to remove those sites from the filtered list for those pupils. Any request to do so should be in request to the Head, and clear reasons for the need must be established and recorded.

Education – Parents

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours.
Parents are guided towards useful education resources in supervising and safeguarding their child's safety outside school.
The School provides information and awareness to parents through seminars and other methods as appropriate

Education & Training – Staff

It is essential that all staff who are granted access to the school network receive e- Safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and overseen by Lousie Reen. E-Safety session, online questions and content is hosted by the following parties: human resources, Dukes, IT-Support and Mr David Zerafa, and recorded as having taken place, as follows.

E-Safety training is made available to staff. This is regularly reinforced. An audit of the e-Safety training needs of all staff with access to the network will be carried out in September 2023 and updated regularly.

All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school the e-Safety Policy and Acceptable Use Policy. This training is overseen and recorded by the Digital lead for their department.

The Digital Leads will receive regular updates through attendance at external training events and/or by reviewing guidance documents released by relevant organisations.

Training – Governors

The e-Safety training for Governance takes place as necessary. The Head is responsible for keeping Governance fully informed. Technical – Infrastructure, Equipment, Filtering and Monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as laid out in the Internet Security Information document.

The Managed Service Provider continually reviews and audits the safety and security of school technical systems, and this audit is supplemented by an external audit and review every three years.

Servers, wireless systems and cabling must be securely located and physical access restricted.

All users are provided with a username and secure password by IT Support. Users are responsible for the security of their username and password.

Internet access is filtered for all users. The firewalls check for an updated filter list daily. If a URL is not on the filter list, the firewall checks the manufacturer's database directly.

This database is updated constantly.

The school provides user-level filtering, allowing different filtering levels for different ages and different groups of users – staff, and DHS pupils, and SLT.

All pupil web access is logged. Staff web access to restricted categories is also logged. Users are made aware of this in the AUP agreement. If a site is blocked by the filter as being inappropriate then access is not allowed. A report on such attempts is sent nightly to the Managed Service Provider and DSL. These are viewed daily.

Given the number of false positives in this logging, the threshold for action is determined by the Managed service provider. Any causes for concern are passed on to the e-Safety officers. Logs are kept for three years.

A system is in place for users to report any actual or potential technical incident or security breach, pupils to the Form tutors or ICT teachers and staff to the DSL and Managed service provider.
Security measures are in place (Appendix: Internet Security Information) to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date anti-virus and anti-malware software.

A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Use of Digital and Video Images

See the Codes of Conduct
When using digital images, staff should inform and educate pupils about the implications of taking, use, sharing, publication and distribution of images. In particular, they should recognise the implications of publishing their own images on the Internet
e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act, and in line with GDPR 2018).

Staff are allowed to take digital / video images to support educational aims, but must follow school policy concerning 'Photography, Videos and other Creative Arts' in the Codes of Conduct

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their agreement.

Pupils' full names may only be used on the intranet or website with parents' permission

Parents are requested to give their permission for the use of Pupils' photographs on the School's Intranet, Website or Social Media as part of their Registration for the School. Where permission is not granted, Charles Walker holds the record and should be consulted before images are used.

Data Protection

The school has a data protection policy which includes electronic data.

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove sensitive personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head Where a member of staff is permitted to download data off site it will need to be password protected.

There are two exceptions where prior approval is not required:
ISAMS, the school's data management system, may be used on personal devices

provided that the device used is secure and password protected.
For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following describes how the school considers the benefit of using these technologies for education outweighs their risks / disadvantages.

These communication technologies are allowed for all adults, and pupils
Mobile phones may be brought to school (however pupils may not use these whilst on the school site, they are handed in to class teachers)
Use of personal email addresses in school, or on the school network. Use of school email for personal emails
Use of messaging apps

These communication technologies are allowed for all adults only:
Use of mobile phones in social time – however this must not be in sight of pupils
Taking photos on tablets/ cameras (this may only be permitted using school equipment)
Use of other mobile devices e.g. tablets, kindles
Use of social media.

Staff may not 'friend' any current or ex pupils.

When using communication technologies, the school considers the following as good practice: 'The School email service may be regarded as safe and secure. Users should be aware that email leaving or entering the school is scanned for viruses, spam and bad language.'

In accordance with the AUP agreement, users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Pupils report to an adult – usually their Form teacher. Staff report to a senior member of staff.

Any digital communication between staff and pupils or parents must be appropriate.

Pupils are provided with individual school email addresses for educational and administrative use. Pupils cannot send emails in any instant. They can only receive emails from specific educational sources where school network permissions have been granted.

Pupils are taught about e-Safety issues within their PHSEE, and Technolgy curriculums, as well as specific school wide E-Safety training sessions.

These cover how to stay safer online, cyberbully, the risks attached to the sharing of personal details and their personal safety in online communication. They are reminded of the need to communicate appropriately when using digital technologies.
On the school website, only school email addresses should be published. Staff should use school email for school business only

.Regarding the use of mobile numbers:

- The sharing and storage of parent phone numbers on personal phones is justified where the context makes it professionally appropriate – for example, for those on school trips – and must be done openly and transparently.
- Staff must not have pupil numbers on personal phones.

Social Media

The school encourages and supports staff in their use of digital technologies, sites and apps in the course of their work (teaching, extracurricular, pastoral) with pupils but requires that any such use is informed and fully consistent with the School's standards and policies. All staff must read and make sure they understand the Codes of Conduct before engaging in any such activity.

- There should be no 'friending' between staff and pupils on social media
- On social sites and apps, closed groups should be used where possible

Unsuitable / Inappropriate Images

The School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. Whilst this list is not exhaustive, the school policy restricts usage as follows:

Pupil Devices – School issued

Where pupils have been given access to a school device for home and school use, all precautionary measures have been taken to ensure its compliance with the school E-Safety and network security.

All pupils (and their parents) who have been given a device must agree to all the school E-Safety IT acceptable use policy. Pupils in year 7 and 8 must also agree to the device user agreement when using our devices or networks. This includes:

Using the device appropriately for school and homework, not attempting to install programs, not accessing inappropriate material such as websites, social media, gaming, gambling, streaming or files, reporting and technical issues with the device (hardware or software related), not accessing, sharing other people's data, not posing as another person, not attempting to bypass any secure features, not accessing or changing any hardware or software settings, not comminating with others or cyber bullying.

Pupil Personal Devices - BYOD (Bring your own device)

Some pupils within the school have permission through the SEN department to use their own personal device. These pupils and their parents must still agree to and follow the school E-Safety and the separate pupil personal device policy.

This includes all previously mentioned elements when connecting to the school network and the following BYOD specific elements:

Pupils can only connect to the specific network setup for BYOD devices

Pupils should only be using their device for learning and not gaming or other non-appropriate software. Any technical issues or damages to a pupil's device (hardware or software) are the responsibility of their parents and not the school.

Educational use of artificial intelligence

The school takes a cautious and pragmatic approach to the use of AI (artificial Intelligence) by acknowledging the advantages of its use in education, including improving student outcomes, streamlining administrative tasks, and reducing teacher workloads.

Only school-approved AI tools should be used, and staff should operate them through school-provided accounts. Transparency is key—documents, emails, and presentations influenced by AI should include clear labels indicating AI assistance. AI-generated outputs must be fact-checked before sharing to prevent misinformation.

When using AI, the school will comply with the set Dukes AI requirements, UK GDPR and data protection regulations. AI tools will be vetted via a risk assessment to ensure data security, and staff must avoid inputting personally identifiable or sensitive information into AI systems. AI should not infringe on intellectual property rights or be used to train generative AI models without appropriate consent.

Staff and governors will receive training on AI's advantages, risks, and ethical considerations. This ensures that both educators and administrators are equipped to use AI effectively and responsibly. Pupils will be educated on the ethical use of AI, helping them develop critical thinking skills and awareness of AI-related risks.

Staff are encouraged to only use AI where appropriate, ensuring it supports their work rather than replacing human decision-making.

For safeguarding this policy highlights the importance of protecting vulnerable learners, ensuring AI does not expose them to undue risks. No pupil will be allowed to use AI without the school and teachers' approval. The school DSL will work with the head of digital learning, to assess AI's impact on pupil safety. Risk assessments, including a school-wide AI inventory, will help monitor and mitigate potential security, legal, and ethical risks.

Any AI-related incidents, such as data breaches or inappropriate outputs, will be reported promptly using the existing safeguarding channels to the DSL and school GDPR officer. Disciplinary action may be taken by SLT for misuse of AI, ensuring accountability at all levels.

Parents and carers will be informed about AI usage in schools through newsletters, online resources, and school E-Safety sessions. This engagement ensures that families understand both the benefits and risks of AI in their children's education and can raise concerns as needed.

User Actions		Acceptable for adults	Acceptable for Pupils	Unacceptable and illegal
Users shall not visit Internet sites, make,	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.			X

post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.			X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.			X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986.			X
	Statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity.	No	No	
	Pornography & adult material.	No	No	
	Promotion of any kind of discrimination.	No	No	
	Threatening behaviour, including promotion of physical violence or mental harm.	No	No	
	Any other information which breaches the integrity of the ethos of the school or brings the school into disrepute.	No	No	
Using school systems to run a private business.		No	No	
Using systems, applications, websites or other mechanisms that bypass deliberately the filtering or other safeguards employed by the school.		No	No	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).		No	No	
Creating or propagating computer viruses or other harmful files.		No	No	
On-line gaming (educational).		Yes	Yes	
On-line gaming (non educational, unless blocked by the system).		Yes	No	

On-line gambling.	No	No	
On-line shopping / commerce.	Yes	No	
File sharing (peer-to-peer).	No	No	
Use of social media.	Yes	No	
Use of messaging apps.	Yes	No	
Creating and uploading of video broadcasts.	Yes	No	
Use of non-school approved AI tools or platforms.	No	No	

Responding to Incidents of Misuse*:* reports of misuse of IT equipment and services may originate from these sources and by these means:

The Managed Service Provider:

- Run weekly filter log reports for the Designated Safeguarding Lead (DSL)
- Through routine examination of firewall and other service logs.
- By alerts raised from desktop monitoring software.
- From materials discovered during routine or other maintenance of School-owned IT equipment – including servers, desktop and laptop computers and mobile devices.
- As a result of observations of unusual patterns of network and storage use.

Through complaints concerning IT related activity made to the School from:

- Pupils
- Parents/carers
- Staff
- Others outside the community

Individuals

- Staff members or pupils who wish to confess to some wrong-doing.

However the incident is reported or discovered there are two broad courses of action that can be taken - depending entirely on whether there is any suspicion of illegality involved or not.

Illegal Incidents

Anyone suspecting that:

- accesses have been attempted to any website containing child abuse images
- accesses have been attempted to any website containing material that breaches the Obscene Publications Act
- accesses have been attempted to any website containing criminally racist material
- accesses have been attempted to any website which contains statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity

- any such materials are themselves to be found on any electronic device - whether owned by the School or not

there has been any incident by electronic means of 'grooming' behaviour must report all allegations, complaints, concerns or suspicions directly to the Head, or, in her absence, to Governance, unless that person is the subject of the concern; those about the Head should be reported to the Governance

Procedure to be followed in the event of an allegation against a member of staff or volunteer of abuse

Including the involvement of the DSL, LADO, Police, Charity Commission, DBS, NCTL or other external agencies, as appropriate.

Concerns, suspicions or allegations of other IT related illegal activity (such as fraud, copyright theft or unlicensed use of software) by a member of staff should also be reported according to the reporting hierarchy outlined above. Such concerns will be managed in accordance with the School's Whistleblowing Policy.

Concerns that relate to the illegal behaviour or actions of pupils or parents/carers (and not staff) should be reported to the DSL or on their absence, the Deputy DSL. The DSL (or Deputy) will follow the Safeguarding and Child Protection Policy and Procedures in reporting any such behaviour to Children's Social Care and/or the Police.

Suspicions of other IT related illegal activity (such as fraud, copyright theft or unlicensed use of software) should be reported directly to the Deputy Head for pupils, and the Head for members of staff.

Safeguarding Incidents

Substantive safeguarding concerns should be reported to Head as per the Safeguarding and Child Protection Policy and Procedures.

Other Incidents

Reports of misuse of IT equipment and services originating from:

- pupils, parents/carers or staff
- admin staff
- individuals

which do not raise safeguarding concerns, or appear to suggest any other kind of illegal activity, should be made directly to the appropriate Line Manager (usually the Head of Department) who will take action as appropriate, consulting the Managed Service Provider as necessary to establish, capture and preserve any relevant data or other evidence.

Misuse of IT equipment and services by pupils or visitors should be referred first to a Deputy Head who may refer to the Head as appropriate

Misuse detected by the IT Support Centre will first be investigated by the Managed Service Provider and evidence gathered. This evidence will then be forwarded to a senior member of staff.

Managed service provider Responsibilities

In the case of a reported incident the e-Safety Officers will take the following actions:

- Evaluate the reports to determine appropriate response.
- To investigate further and to provide more evidence.
- To initiate a response to the incident according to normal disciplinary procedures for both staff and pupils.
- To log the incident in the e-Safety Incident Log.
  Following the conclusion of any incident the Managed Service Provider will log the incident; review the incident to determine if any modification to policy or practice is required; and brief the Head on all incidents at the next meeting

IT Investigations

Where directed by the Head or DSL or by an external agency such as the Police, the Managed Service Provider will undertake further investigative actions. These may include:

- Detailed examination of firewall, filter, mail relay and other security logs - and the extraction therefrom of references to activity associated with the incident in question
- Examination of materials stored on the School's storage networks - taking copies of any items associated with the incident in question.
- Remote examination of School desktop and laptop computers - and the gathering of relevant evidence therefrom, including the copying of materials or the taking of screen-captures as required.
- Examination of the contents of School email mailboxes, including sent and deleted items - and the extraction of messages and materials relevant to the incident in question.

The requiring of staff to return School-owned mobile devices for investigation. These investigations will be carried out by the Managed service provider.

Unsuitable materials will be copied and may then – under the direction of an appropriate authority - be deleted from storage, mailboxes or computers.

At the culmination of the investigation a report on all materials and references found - detailing the processes followed - will be passed on to the Head; names will be redacted as appropriate from all such reports in accordance with confidentiality requirements.

Should any of these investigations uncover materials or accesses for which there is any suspicion of illegality the Managed Service Provider will immediately suspend any further inspection, reporting the matter in accordance with the procedure above (illegal incidents) or to the Police (if already involved) and awaiting direction from them. The Managed Service Provider will also assist with the recovery of School-owned equipment

such as desktop and laptop computers and mobile devices as required by the relevant authorities.

The Managed Service Provider will only examine the contents of devices not owned by the School with the prior agreement of the pupil and/or his parents.

Appendices

Pupils' AUP
Staff AUP
Internet Security
Information
Protocols for monitoring and reporting
Information sent to parents
Visitors' AUP

Devonshire House Preparatory School

Devonshire House Preparatory School

ICT Acceptable Use Policy for Pupils

This policy is for the whole school including EYFS

ICT Acceptable Use Policy for Pupils

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The School provides both networked, desktop computers and wireless access to the internet through its own filtered connection.

Personal safety and responsibility

- I understand that the School will log and monitor my use of computers, devices and my digital communications;
- I will keep my school username and password safe and secure. I will not share it, nor will I try to use another pupil's or staff member's username and password. I understand that I should not write down or store passwords where it is possible that someone may steal them;
- I will not leave any school device, or device connected to the school network, logged on for others to use;
- I will not give out personal information about myself or others that could be used to identify me, my family or my friends (e.g. addresses, email addresses, phone numbers, information about the school or my age or the age of another pupil) unless a trusted adult has given me permission;
- I will never arrange to meet someone I have only ever previously met online unless I take a trusted adult with me;
- I will only use school computers and devices as directed. I will not use school devices for on-line gaming, on- line gambling or internet shopping and I will not visit sites I know to be unsuitable;
- I understand that some websites and social networks have age restrictions and I will respect this;
- I understand that once something is posted online or written in an email it has a permanence that is not like something that is said. It can be repeated, is searchable and can be copied out of context. I understand that I have to take responsibility for my actions online and I should consider my reputation, the reputation of others and the reputation of the School.
- If I see anything unpleasant or inappropriate or I receive a message I do not like, I will not respond but I will save it and talk to a trusted adult as soon as possible;

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language. I will not send messages either anonymously or pretending to be someone else and I will not send group messages needlessly;
- I will not take or distribute images of anyone without their permission;
- I will edit or delete my own files only and not view, or change other people's files without their permission

Device security

- I will not use any personal devices (mobile phone, USB device, laptop , iPad etc.) in school;
- I will not try to upload, download or access any materials which are illegal, or encourage illegal, extremist or terrorist activity, or which may cause harm or upset to others, nor will I try to use any programs or software that might allow me to bypass the filtering systems in place to prevent access to such materials;
- I will report immediately any damage or faults involving school equipment or software, however this may have happened;
- I will report any actual or potential technical incident or security breach to my teacher or to a member of staff;
- I will not open a hyperlink in any email or attachment to an email if I have any concerns about it or think it may contain a virus or other harmful program;
- I will not install, attempt to install or store programs or software on any school device, nor will I try to alter the computer settings.

Sanctions

- I understand that if I fail to comply with this Acceptable Use Policy Agreement I will be subject to disciplinary action. This would include involvement in incidents of cyber-bullying or any inappropriate behaviour that is covered in this agreement, when I am in or out of the School and where it involves my membership of the school community.

I agree to comply with the rules and regulations set out in the Devonshire House School ICT Acceptable Use Policy Agreement for pupils.

Parent or Guardian

As the parent or guardian of this pupil, I have read the **ICT Acceptable Use Policy for Pupils**.
I understand that this access is designed for educational purposes and that Devonshire House Preparatory School has taken available precautions to eliminate controversial material. However, I also recognise that it is impossible for Devonshire House Preparatory School to restrict access to all controversial materials and I will not hold them responsible

for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting.
I hereby give permission for my child to use the Internet and Learning platform for educational use.

Pupil's name:

Parent or Guardian's name (please print):

Parent or Guardian's Signature: .....

Date: .....

Devonshire House Preparatory School

Devonshire House Preparatory School

ICT Acceptable Use Policy for Staff

This policy is for the whole school including EYFS

ICT Acceptable Use Policy for Staff

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought you should be putting into practice much of this policy.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community must take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

***This Acceptable Use Policy is intended to ensure**:*

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use when in school, when using school systems and equipment and when connected to the school network
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of ICT in their everyday work

Access to ICT is made available to staff to enhance their work and to enhance opportunities for pupils' learning, and the school expects staff to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.
- In any interactions with pupils I will ensure appropriate use of ICT.

- I confirm that I have read and understood the Devonshire House School e-Safety Policy.

For my professional and personal safety:

- I understand the school will monitor my use of its ICT systems and networks. I understand that the rules set out in this agreement also apply to use of school ICT systems out of school, and to the transfer of personal data out of school
- I understand that the security of my account is my responsibility and that I should log on only as myself;
- Keep my login details private and make them secure;
- Not leave any device logged in and accessible to others.
- I will report any actual or potential technical incident or security breach to the Managed Service Provider.
- I will immediately report any illegal, inappropriate or harmful material I become aware of when in school or connected to the school network:
- Material that appears to originate from sources external to the School should be reported to the Managed Service Provider;
- Material that appears to have been sent or circulated by a pupil or parent/carer should be reported to the Designated Safeguarding Lead (DSL) (or in their absence the deputy DSL);
- Material that appears to have been sent or circulated by a member of staff (including a temporary member of staff or volunteer) should be reported to the Head.

I will be professional in my communications and actions when using school ICT systems at school, when using school ICT systems and equipment or when connected to the school network:

- I will ensure that when I take and / or publish images of others I will do so in accordance with the school's policy on the use of digital / video images.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Any use that I make of chat and social networking sites will be in accordance with the guidance given in the Codes of Conduct.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I understand that the school ICT systems are primarily intended for educational use.

The school has the responsibility to provide safe and secure access to ICT:

- I will not open any hyperlinks in emails, or any attachments to emails, unless the source is known and trusted.
- I will not try to upload, download, or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for

school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access such materials.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Data Protection Policy.
  I understand that data protection requires that any staff or pupil data to which I have access must be kept private and confidential

- I will immediately report any damage, loss or faults involving school equipment or software to IT Support.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this AUP Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises.
- I am aware that emails may be disclosed as evidence in court and that, even if deleted, copies may exist on a back-up system
- I understand that if I fail to comply with this AUP Agreement, I could be subject to disciplinary action.

I agree to comply with the rules and regulations set out in the ICT Acceptable Use Policy Agreement for staff.

Name: .....

Date: .....

Internet Security Information

Internet security is a branch of computer security specifically related to the Internet. The Internet represents an insecure channel for the exchange of information and for access to online services. By its nature it carries a high risk of intrusion or fraud, as well as the possibility of inadvertent or malicious abuse by those accessing it. The objective of the schools' security approach is to establish rules and measures to protect against attacks from the Internet and to prevent abuse from within the School, whilst at the same time balancing these risks against the requirement to ensure that members of the community have the widest possible access to internet resources in order to enhance teaching and learning, or for administrative use.

Aim.

The aim of this appendix is to highlight the risks associated with internet usage and identify the methods used to mitigate these risks. As will be seen from the technical details below, the security tools in use at the School are extremely flexible.

Policy Control.

Security policy is ultimately determined by SLT for each part of the School. They have responsibility for oversight of Internet Security Policy. The Managed Service Provider and his staff are responsible for implementation and monitoring of the policy, and for reporting breaches thereof.

Incident Reporting.

Substantive safeguarding concerns should be reported to the Head. Concerns which are not of a safeguarding nature should be reported in the first instance to the appropriate Deputy Head.

The following risks and mitigations have been identified

:**Risks related to Internet Use**	**Details**	**e-Safety implications**	**Mitigation**
Access			
Unauthorised access - by those within and outside the School	Use of School systems without permission	Yes	The School's network and systems can only be accessed by use of a network account - identified by a username and password. Network account details are only handed over in person after an induction.
Security of network accounts	Insecure passwords - sharing of accounts - revealing account details - attempting to use another's account	Yes	Strong passwords are enforced and staff and pupil inductions reinforce the importance of network account security - and the users' responsibilities therefore. Forgotten passwords will only be reset by the Managed service provider .
Accountability - monitoring	Attempts to avoid account monitoring		Role based or shared network accounts are deprecated unless tied to an accountable individual. All logons are recorded in

			multiple event logs and databases.
Accountability - AUPs	Non-compliance with School policies	Yes	The School's Acceptable Use Policies are signed electronically annually.
Attacks on infrastructure			
Viral attacks	Viruses, worms, Trojans		The School runs an application layer firewall by Smoothwall. The firewall provides antivirus, threat protection and URL filtering services. All of the School's servers and desktop systems run additional endpoint antivirus software for protection against Malware, Viruses and Ransomware. Currently we use Sophos Intercept X.
Malware	Malware, spyware, adware, ransomware		Covered by Smoothwall threat protection and service. We are also covered by Sophos Intercept X on all Server and PC's.
Denial of service attacks	Attempts to interfere with legitimate traffic by flooding the network		The Smoothwall firewalls prevent all currently known DoS attacks. The configuration of the School's networks and of the security rules on the firewalls further mitigates this and other attacks.
Exploitation of software vulnerabilities	Exploitation of known vulnerabilities in operating systems and applications		Covered by the Smoothwall threat protection service. Inside the School systems are protected by group policies such that users cannot access system components.

Risks related to Internet Use	Details	e-Safety implications	Mitigation
Attempts to access infrastructure equipment and services	Attempts to log on to or otherwise interfere with infrastructure equipment such as firewalls, switches and routers		The School's network is configured such that management access to infrastructure items is only possible by IT staff.
Installation or use of unauthorised software on School systems			School systems are locked against the installation or re-configuration of software by users.
Connection of poorly configured personal devices	Connection of devices not owned by the School that may be infected with virus or worms, or have badly configured network connections		Personal devices may not be connected to the wired network without permission of the Managed Service Provider. The wireless network is configured as a 'sandbox'. All other School systems are protected from it.
Hacking, cyber espionage from outside the School			Covered by Smoothwall threat protection service.
Use of hacking tools within the School	Keyloggers, password crackers, promiscuous packet capture		
Antisocial Use			
Bandwidth hogging	Use of applications the consume unreasonable amounts of bandwidth		The Smoothwall firewalls are configured to prevent the use of heavy bandwidth applications such as peer to peer files sharing. Network bandwidth use is constantly monitored to identify abuses.

Running unauthorised services	Connection of a device to the School network that advertises unauthorised websites or other Services		The firewalls are configured in such a way that only authorised sites and services can be publicised from the School's network to the Internet. A variety of network scanning tools are used to identify other rogue services.
Storage			
Security of user files and resources held on School systems	Attempts to access to user's files and resources without permission	Yes	Access to the School's storage networks is tightly controlled by permissioning based on the users' network accounts. This gives direct accountability and security.

Risks related to Internet Use	**Details**	**e-Safety implications**	**Mitigation**
Integrity of user files and resources	Attempts to alter or delete others users' files and resources		File security makes it most unlikely that a user could maliciously damage another user's files, but in the event of such happening the Managed Service Provider can restore from routine backups. The backup regime covers all School storage systems on a nightly basis and there are additional mechanisms to allow users to recover their own files should they become lost or damaged.
Security of system and administrative resources	Attempts to access the system or School administration resources without permission		Access to the School's storage networks is tightly controlled by permissions based on the users' network accounts. This gives direct accountability and security

Integrity of system and administrative resources	Attempts to alter or delete system or School administration files and resources		In addition to the mechanisms defined above all School databases are backed up to multiple locations to provide increased resilience
Unacceptable or inappropriate storage of personal data	Use of the School's storage networks in an unauthorised or insecure manner for personal data		The Managed Service Provide rhas access to all file systems and monitors broad patterns of use constantly. Suspicious traffic patterns are investigated in depth
Access to copyright materials	Making accessible materials in breach of copyright - e.g. - outside the School		The School's streaming media servers are configured to prevent access to materials thereon that might breach copyright. The staff AUP states that work protected by copyright will not be downloaded or distributed for any school work, and use of any original work by others requires their permission. Pupils receive instruction in the use of copyright and otherwise licensed material.
Introduction of inappropriate or illegal materials onto School systems across the network from other public networks, from personal devices, from removable media	The copying or downloading of inappropriate or illegal materials onto School computers or network storage solutions		The filters are configured to prevent access to and the downloading from Internet sites that have been categorised by the filter manufacturer. Attempts to access blocked sites are recorded and daily reports sent to the

			Managed service provider .
Email			

Risks related to Internet Use	**Details**	**e-Safety implications**	**Mitigation**
Unacceptable/inappropriate use of email	Unprofessional conduct - use of unacceptable language - inappropriate email targeting - use of School systems for commercial purposes	Yes	Office365 has strong filtering inside it that is configured to block inappropriate use of language.
Antisocial use of email	Sending of inappropriate or unauthorised bulk emails		Office365 has strong filtering inside it that is configured to block inappropriate use of language.
Email attacks	Spam, mail-bombing and phishing attacks, use of botnets		The Sophos Intercept X software includes antivirus and antispam filters and can protect against a wide variety of mail based attacks.
Relaying - anonymous and otherwise	The use of School email system to forward messages to other external mail systems	Yes	The mail relays are configured to prevent the relaying of emails by any system on the School's network other than authorised mail servers.

Bullying		Yes	The Smoothwall software maintains a log of messages sent and received that can be used for diagnostic and forensic purposes. Smoothwall can be used to flag up immediately to the Managed Service Provider any situation where a school computer is used to type or display any word on a specified trigger words list, which includes words associated with bullying and trolling.
Accidental exposure of data	Careless use of email resulting in data being send to the wrong recipient		Internal emails can be recalled by the user, and they can be deleted from mailboxes en masse by IT. Staff induction includes advice on the careful use of email.
World Wide Web			

Risks related to Internet Use	**Details**	**e-Safety implications**	**Mitigation**
Access to unsuitable materials	Accessing materials and websites that are inappropriate in a school environment	Yes	The filters are configured to prevent access to and the downloading from Internet sites that have been categorised by the filter manufacturer. Attempts to access blocked sites are recorded and daily reports sent to the Managed Service Provider and his deputy. Substantive safeguarding concerns

			would be reported to the Head as per the Safeguarding and Child Protection Policy and Procedures. Concerns which are not of a safeguarding nature would be reported in the first instance to the appropriate line manager (relevant Deputy Head).
Access to terrorist or extremist propaganda	Accessing or generating statements or images which endorse, condone, or incite illegal, extremist or terrorist activity	Yes	As above, plus Smoothwall software is used to flag up immediately to the Managed Service Provider any situation where a school computer is used to type or display any word on a specified trigger words list, which includes words associated with extremism or radicalisation.
Access to illegal materials and services	Accessing child abuse materials - race or hate crime materials - materials that breach the Obscene Publications Act - fraudulent or copyright materials, unlicensed software or services	Yes	Smoothwall is used to detect, track and block illicit material.

Access to unwanted materials	Inadvertent viewing of unsuitable materials	Yes	The filters are configured to prompt staff before allowing access to a range of subject categories that - whilst not deemed unsuitable - are considered to require caution.
Gaming and gambling		Yes	See above.
Excessive use of the Internet		Yes	This is a pastoral issue.

Risks related to Internet Use	**Details**	**e-Safety implications**	**Mitigation**
Running unauthorised websites	The publicising within or outside the School of websites purporting to have official backing without permission	Yes	The firewalls are configured in such a way that only authorised sites and services can be publicised from the School's network to the Internet. If unacceptable sites outside the School are reported the IT Manger will inform the Head.
Social Networking			
Inappropriate or unsafe use of social media	Inappropriate communications between adults and children - exposure to grooming - awareness of audience – control of permissions - sensitivity regarding personal data - regard for reputation	Yes	The School's policies and guidance on the safe use of social media are foregrounded in safeguarding training. Pupils are given extensive guidance through the ICT curriculum regarding the safe use of social media. Software is used to flag up immediately to the Managed Service Provider any situation where a school computer is used to type

	(school and personal)		or display any word on a specified trigger words list, which includes words associated with grooming, bullying, trolling and radicalisation.
Antisocial use of social media	Trolling, abusive messaging	Yes	See above. The School's Anti- bullying Policy also applies.
Inadequate privacy settings	Allowing public access to personal information through inadequate knowledge of security settings	Yes	See above.
Bullying		Yes	See above. The School's Anti- bullying Policy also applies.
Exposure to social network based attacks	Social engineering, fake offers, manual sharing scams, 'like' jacking, fake plugins, fake apps	Yes	See above.
Intranets and external websites			

Risks related to Internet Use	**Details**	**e-Safety implications**	**Mitigation**

Publishing of unsuitable materials	The publishing on School websites and intranets of unsuitable, inflammatory or otherwise unauthorised materials		The School's content management solution - Firefly - logs the creators and editors of content, who are identifiable through their network accounts. The webmasters for these sites have control over permissioning.
Bringing the School into disrepute	The publishing on websites or social media outside the School of materials or comments that damage the reputation of the School		
Personal and Mobile Devices			
Dangerous or careless use of resources personal or mobile devices	Use of personal or mobile devices in a manner that could cause a breach of the School's AUPs - inadvertent access to personal data or resources through lack of understanding	Yes	For School owned devices, safeguarding training is given as part of the device induction. A Conditions for Loan form must be signed by the recipient of the device which covers safeguarding requirements.
Theft or loss of personal devices	Loss of School owned devices - loss of personal data contained thereon	Yes	School devices are covered by a signed agreement as to the user's responsibilities for the device.
Digital Literacy			
Abuses resulting from ignorance	Breaches of School policies through lack of knowledge of IT systems	Yes	Staff training and INSET aims to raise staff awareness of the Internet and its uses. The ICT curriculum does the same for Pupils.

Unsafe practices caused by lack of knowledge	Lack of understanding of how Internet services such as synchronisation of cloud storage and social networks operate can result in unsafe use of the Internet	Yes	See above.

Risks related to Internet Use	**Details**	**e-Safety implications**	**Mitigation**
Circumvention of the School's security mechanisms			
Anonymous proxies	Attempts to access websites and services otherwise prohibited from the School's network by bypassing the School's security systems	Yes	Known anonymous proxies are blocked by the firewalls.
Http tunnelling	Attempts to bypass security systems by tunnelling through secure connections	Yes	We implement SSL decryption for pupils with one or two exceptions in selected categories, such as banking and shopping.
Masquerading	Attempting to use another person's identity on the Internet - e.g. - as email sending address	Yes	Extensive logs are maintained on all of the School's platforms that can be used forensically to trace such wrongdoing.
IT Service Issues			

Incorrectly or poorly configured systems	Security loopholes in School networks and systems as a result of poor design or configuration		The ITSC has a considerable range of experience in the design and maintenance of secure networks and systems. This is augmented by ongoing training and research. In addition, internal and external penetration tests are carried out on an annual basis. IT support also carry out weekly tests on systems and infrastructure.
Out of date software versions	Updates and security hotfixes not applied in a timely fashion		All School systems are updated at the earliest possible point - depending on the urgency of the hotfix. Central management solutions roll out most updates automatically - except in circumstance where so to do might compromise the service provision.
Out of date threat databases	Antivirus, threat and URL filtering databases not being updates on a regular basis		Antivirus, threat protection and URL filtering databases are updated automatically on a nightly basis.
Inadequate IT staffing	Insufficient or poorly trained IT staff resulting in poor systems design and maintenance		The Managed Service Provider is highly experienced and has an appropriate annual training budget.

Risks related to Internet Use	Details	e-Safety implications	Mitigation
Future Threats			
As yet unknown Internet threats			The Managed Service Provider is charged with ongoing research into new and evolving Internet and other security related issues.

E-Safety Protocols for Monitoring and Reporting

These monitoring and reporting protocols are to be read in conjunction with the e-Safety policy

Responsibility	Policy Reference	Requirement	Frequency	Dates	Remarks
Managed service provider	-Schedule for Development /Monitoring/ Review -e-Safety Group (ICT Committee) Roles and Responsibilities	Report on e-Safety for SLT	Termly	Summary of preceding term's e-Safety issues presented early each term to SLT	Standing item at SLT beginning of each term to include Summary of e- Safety incidents. E-Safety Staff Training report.
Managed service provider and SLT	e-Safety Group	Report on e-Safety for Governance	Annually	Last Governance Meeting of the Summer Term	

Devonshire House Preparatory School

Sharing, Distribution and Publication of Images of Pupils
This policy is for the whole school including EYFS

Dear Parents,

Sharing, Distribution and Publication of Images of Pupils

I am writing to explain the School's policy regarding the use of the sharing, distribution and publication of images of pupils. I hope that you will feel able to endorse the same level of trust in this area that you afford to us in all other areas of our care for your child at Devonshire House School.

We like to use photographs or videos to celebrate the achievements of our pupils and to allow pupils, staff and parents to enjoy memories of past events. We believe that by taking proper precautions any risk to individuals can be made very small and that using images of pupils should continue in line with the policy set out below.

Photographs, digital images or videos of pupils may be taken either at the School or when pupils are involved in organized activities off site. We use some of the images in school publications, such as the Newsletter, on the intranet, or on the website or on School social media. CCTV is located around the School but is not installed in classrooms, changing rooms or toilet areas. All surveillance within the School is overseen by a data controller registered with the Information Commissioner's Office.

Parents and family members are welcome to take photographs or videos of school events which may include images of other pupils. To respect the privacy of others and in some cases for protection purposes, these images should not be made publicly available. Copyright issues may prevent the School from permitting the filming or recording of some plays or concerts. A reminder will be printed in the programme of events where issues apply. Flash photography can disturb others in the audience or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events.

The School's Policy

We comply with the Data Protection Act and the requirements of the Information Commissioner's Office and we follow the advice given by the Department for Education which states: "If the pupil is named, avoid using the photograph. If the photograph is used, avoid naming the pupil". Where it is deemed necessary or desirable to deviate from the above policy (for example, in an article celebrating a particular pupils achievements) we will always seek specific parental consent before publication.

We would also seek parental consent before publishing any images in the newspaper or magazine.

If you have any concerns regarding the information in this letter, please do not hesitate to get in touch. If I do not hear from you I will assume that you are happy for the School to use static or video images of your child, unidentified by name, in school publications (e.g. newsletter, magazine, website, intranet, and social media).

We are aware that some parents have already expressed their wish that their child not be included in published material and that names are already on file.

Parental Consent Form – Use of Photographic Images

This policy is for the whole school including EYFS

Parental Consent Form – Use of Photographic Images

Child's name (please print):
May we take static or video images of your child and use them, unidentified by their name, in school publications (prospectus, magazines, website, intranet etc.)?

Yes ☐ No ☐

I understand that if it is deemed necessary or desirable to use the name of my child alongside their photograph, my permission will be sought before publication. The School will also seek my consent before any images of my child are published in newspapers or appear in other news media.

Declaration

I have read and understood the School's policy regarding the use of photographs of pupils. My decision on whether to give consent will remain valid throughout my child's

time at Devonshire House School unless I notify the School to the contrary in writing. If I or members of my family take photographs or video recordings at a school event, I promise that these will be kept for family use only.

Parent 1

Name:

Relationship to Child:.....

Signature: .....

Date:

Parent 2

Name:

Relationship to Child:.....

Signature: .....

Date:

Visitors – AUP – Acceptable Use Policy

Last Reviewed	2025
Reviewed By (Name)	David Zerafa
Job Role	Digital Lead
Next Review Date	2026

This document will be reviewed annually and sooner when significant changes are made to the law. Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

Introduction

As a visitor / contractor to Devonshire house you may be given access to school devices or networks to aid the provision of your services or your support to pupils and staff of the school. You are required to sign this document prior to accessing the school systems.

All visitors to school are expected to abide by relevant school policies. Special consideration should be given to the following:

· Data Protection Policy

· IT Security Policy

· IT Security & Acceptable Use Policy

· Bring Your Own Device (BYOD) Policy

· Online Safety Policy

IT Acceptable Use Standards

All Users must:

1. Protect school IT resources by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
2. Protect individuals from harmful or inappropriate material accessible via the Internet or electronic media.
3. Protect the confidentiality of individuals and of school matters and safeguard Users by complying with relevant legislation, including, but not limited to:
    - Data Protection Act 2018 and General Data Protection Regulation
    - Privacy and Electronic Communications Regulations
    - Copyright, Designs and Patent Act 1988
    - Computer Misuse Act 1990
    - Counter-Terrorism and Security Act 2015 (encompassing the "Prevent Duty")
    - The Regulation of Investigatory Powers Act (RIPA) 2000
    - Waste Electrical and Electronic Equipment Regulations 2006, the Environmental Protection Act 1990, the Waste Management Regulations 2006.
    - The Department for Education Digital and Technology Standards for Schools and Colleges
    - Keeping Children Safe in Education (KCSIE)

Users should understand and adhere to their signed Acceptable Use Agreement.

Agreement Statements

1. Any observations, incidents, or conversations taking place during my time in school will be kept confidential.

2. I understand that it is my responsibility to support the safeguarding of pupils and other staff. If I have any Child Protection or Safeguarding concerns, or if I am asked to do something, or see something I consider not best practice, I will report this to the school Safeguarding Lead (Louise Reen).

3. I understand the importance of upholding my online reputation, my professional reputation, and that of the school, and I will do nothing to impair these. I will conduct myself in a professional manner, including professional dress and always using appropriate language.

4. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school. I will not contact or attempt to contact any pupil in any way other than school-approved and school-monitored ways.

5. I will not store school-related data on personal devices, storage, or cloud platforms.

6. I will not access, attempt to access, store, or share any data which I do not have express permission for.

7. I will not share any information about the school or members of its community gained during my visit, verbally, electronically, or via social media in any way, or on any platform, except where relevant to the purpose of my visit and agreed in advance with the school.

8. I will not take photographs or videos whilst on site unless the purpose has been communicated to senior leaders and prior permission has been granted. (e.g., to take photos of equipment or buildings)

9. I understand that school systems and users are protected by security, monitoring, and filtering services, and that my use of school devices and systems can be monitored/captured/viewed by the relevant authorised staff members.

10. School-owned devices, networks, cloud platforms or other technology, will be used exclusively for the purposes to which they have been assigned to me, and not for any personal use. I will not attempt to bypass security or monitoring and will look after devices I have been given authorised use of.

11. When using my own devices on school premises or accessing school systems / platforms, I will ensure I take appropriate steps to safeguard and secure my device.

12. USB sticks / pen drives are not authorised unless permission has been sought from the school IT Support Team (these are a considerable security risk from outside the school network.)

13. I will report any suspected security incidents, notifications, or security alerts from antivirus systems, firewalls, or malware protection, promptly, to the school IT Support Team.

I understand that breach of this agreement may lead to appropriate immediate termination of any contracts and, when necessary, referral to other relevant authorities.

I have read, understood, and agree to the conditions of the acceptable use agreement for IT and the Internet of Devonshire House.

Signature: _____ Name: _____

Devonshire House Preparatory School

Organisation: _____ Date / Time: _____

I approve this user to be allocated credentials for school systems for the purpose of:

_____

Signature: _____ Name: _____

Role: _____ Date: _____

Amend a complete list of systems the user has been given access to and the level of access provided.

Users should also be advised how to report and respond to suspected incidents.

Key contacts to be provided to the user:

Role	Name	Email
Headteacher	Henry Keighley-Elstub	hmpa@dhprep.co.uk
Safeguarding Lead	Louise Reen	dephdjs@dhprep.co.uk
Deputy Safeguarding Lead	Lucy Peacock (lower school) Jude Swailes (upper school)	l.peacock@dhprep.co.uk j.swailes@dhprep.co.uk

Devonshire House Preparatory School

Visitor / Contractor Concern Form

Part 1 - to be completed by the person raising concern	
Name of Visitor / Contractor:	
Date and time:	
Summary of concern and any known details:	
Does it involve any individuals?	
If so, can you provide names?	
Any action taken so far: *Please include other staff members aware of the issue and any witnesses.*	
What type of concern is this?	Safeguarding Concern Security Incident Unauthorised Use Illegal Activity Breach of policy

Please pass this concern form to the Headteacher.

Part 2 – to be completed by Headteacher	
Date and time received:	
Outcomes and Actions *Record any contact with Action Fraud / Police Cyber Protection Officers / IT Provider etc.* *If this information is transferred to CPOMS / MyConcern or similar system, state this and add any reference.*	

In the case of safeguarding concerns this record should be retained by the DSL. Part 3 – to be completed by DSL	
Date and time received: DSL initial:	

Devonshire House Preparatory School

CP concern: YES / NO Starting Point referral: YES /NO	
Is this a concern under Prevent: YES / NO If YES: Complete Prevent Risk Indicator Checklist	
Further actions taken: *Record all strategies agreed including school based ones, and record an outcome including evidence of referrals/agreement with agencies.*	
Have parents/carers been contacted? YES / NO	
If NO, provide justification here: *In all cases except where there is clear evidence of putting a child at immediate risk, parents/carers should be contacted.*	
Feedback to Referrer YES/NO Date closed:	