DAVID GAME COLLEGE

**Document No. 29**

# ONLINE SAFETY POLICY 2022-2023
## (Inclusive of Cyber Bullying, Acceptable Use and Social Media)

*This document which applies to the whole college inclusive of boarding is publicly available on the college website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the college office.*

**Scope:** All who work, volunteer or supply services to our college have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal college hours, including activities away from college. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the Policies Register.

**Legal Status**: Complies with The Education (Independent School Standards) (England) Regulations currently in force.

**Monitoring and Review:** These arrangements are subject to continuous monitoring, refinement, and audit by the Co-Principal, who will undertake a full annual review, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements and it will be made available to them in writing or electronically.

Reviewed: March 2022
Next Review: March 2023

Signed

David Game
Co-Principal and Founder

John Dalton
Co-Principal

**Aims:** David Game College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, proprietorsand parents or guardians
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**Rationale:** This policy has been authorised by the Leadership Team of the College and addresses the College's response to promoting a safe and tolerant environment for its students. Online safety is a running and interrelated theme when devising and implementing our wider College policies and procedures, including ourSafeguarding & Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy.We consider how we can promote online safety whilst developing our curriculum, through our staff training, and also through parental engagement. Technology use is a ubiquitous part of peoples' lives and this is also true for students and staff within education. This policy gives a broad overview of how the College will attempt to make sure that students are not exposed to material content that may put them at risk. Other specific policy-guidance documents have been produced for both students and staff in relation to theacceptable use of technology.

The following is a list of possible risks students may face in their access to technology:

- Access to illegal, harmful or inappropriate images or content
- The risk of being subject to grooming by those whom they contact on the internet
- Inappropriate and unsafe communication with strangers
- Cyber bullying
- Access to pornographic material
- Access to extremist material that could lead to radicalisation of students
- Access to unsuitable video or gaming sites
- Sites that encourage gambling
- Illegal downloading of material that breaks copyright laws
- Unauthorised access to/loss of/sharing of personal information

The above risks can be realised through a wide range of technologies, including:

- e-mail
- Smart phones, tablets and laptops, etc.
- The Internet (web)
- Social networking sites; Twitter, YouTube, Facebook etc.
- Gaming sites
- Blogs, instant messaging, chat rooms, message boards, virtual learning environments
- Webcams, video hosting sites
- Photography

**Legislation and guidance**

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent College Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Students Safe in Education* (KCSIE) *Information for all Colleges and Colleges* (DfE: September 2021) incorporates the additional statutory guidance,
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard Students* (WT) (HM Government: September 2018) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for* *England and Wales* (March 2015) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for Colleges and childminders (June 2015)* and *The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note ForColleges (DfE )*
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and College staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for College leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in Colleges.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in Schools (DfE: 2019)
- The policy also takes into account the National Curriculum computing programmes of study.

The following legislation and guidance should be considered:

- Data Protection Act 1998
- DFE Guidance - Keeping Children Safe in Education (2015) and Working Together to SafeguardChildren (2015)
- Human Rights Act 1998
- Regulatory of Investigatory Power Act 2000
- Computer Misuse Act 1990 – Police and Justice Act 2006
- Prevent Duty – Counter-terrorism and Security Act 2015
- Obscene Publications Act 1959, Protection of children Act 1988, Criminal Justice Act 1988

**Liability of the College:** Unless specifically negligent under the terms of this policy, the College does NOT accept any responsibility to the parents or students for a problem caused by a student's use of mobile phones, email, or the Internet while at the College.

**Roles and responsibilities:** The Co-Principals, working in conjunction with our IT managers, are responsible for ensuring the online safety of the College community. Our Head of IT will take operational responsibility for online safety in the College, but the overall responsibility will fall on the senior management for making sure that policy is enforced and that the necessary checks, filters and monitoring are in place. It is the College responsibility to ensure that students are safe from cyber bullying both within and outside the College community and that appropriate steps are taken if an incident occurs. The Leadership Team will also review online safety and theacceptable use of technology in the College during their regular meetings.

The Head of IT will act as the online safety officer with the assistance of our Data Protection Officer. He along with the Leadership team will also be responsible for staff training and that staff are aware of the guidance notes to staff and have signed them accordingly. Specifically, staff must be aware that digital communication with students should be on a professional level and only carried out using official communications systems. In addition, online safety must be embedded in all aspects of the curriculum and other College activities. Students should have read, understood and signed the guidance notes on online safety. Parents will be copied with student guidance notes.

Our Head of IT is also the network manager and he has a specific duty of care to ensure that suitable controland filters are in place and that the system is secured and risk-assessed, based on College policies.
In particular, the IT Head should ensure that:

- All users have clearly defined access rights to the College IT systems
- Servers, wireless systems and cabling are securely located and physically protected and haveaccess restrictions
- All work stations are protected with up-to-date virus software
- Personal or student data cannot be sent over the Internet or taken off the College site unless safelyencrypted
- All users are provided with a user name and password
- Regular reviews of the network system are taken to examine vulnerabilities and risks
- Staff must be very careful when taking student images, even if they support educational aims. Any images taken for educational purposes can only be done so with the parents' and students' prior permission (written)
- Staff and students cannot publish images of others without their permission
- Students should be fully aware of their responsibilities and limitations in relation to images over social media by reading the student guidance notes
- Sensitive personal data should not be communicated by e-mail, but can be sent across D11 systems
- Staff must not include any defamatory comments in any emails
- Staff CANNOT electronically communicate with students inside or outside College unless they are using the designated College system and all communications are subject to inspection and review
- The use of social networking sites within the College is only allowed in appropriately controlledsituations and in support of legitimate curriculum activities
- Students and staff must report any inappropriate material about them or others online which couldbring the College into disrepute

**The Proprietor:** The proprietor at David Game College, the Directors and the Senior Team, have overall responsibility for monitoring this policy and holding the Co-Principals and vice Co-Principals s to account for its implementation. The proprietor will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL) who is Nedaa Belal nedaa@davidgameCollege.com. The Co-Principal who oversees online safety on behalf of the Senior Team, is John Dalton (j.dalton@davidgameCollege.com) who with the Senior Leadership Team, senior team, will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on **acceptable use agreement** (to be signed by all staff members) ofthe College's IT systems and the internet (see appendix 2)

They are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

**The designated safeguarding lead**: Details of the College's designated safeguarding lead (DSL) and deputy, Julia Cushnir (j.cushnir@davidgameCollege.com) as potentially our designated prevent lead, John Dalton (j.daltonlsp@davidgameCollege.com), are set out in our child protection and safeguarding policy also ourprevent policy. The DSL takes lead responsibility for online safety in College, in particular:

- Supporting the Co-Principals in ensuring that staff understand this policy and that it is beingimplemented consistently throughout the College
- Working with the Co-Principals , IT manager and other staff, as necessary, to address any onlinesafety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately inline with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College's **behaviour policy**
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff ononline safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to one of the Co-Co-Principals s This list is not intended to be exhaustive.

**The IT manager:** The IT manager, Zed Abaderash, **zed@davidgameCollege.com** and his deputy our data protection officer (DPO), Alexandra Raen**, dpo@davidgamecollege.com** are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basisand keep students safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Ensuring that the College's IT systems are secure and protected against viruses and malware, andthat such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately inline with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College's **behaviour policy**

This list is not intended to be exhaustive.

**All staff and volunteers:** All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the College's IT systems and the internet (appendix 2), and ensuring that students follow the College's terms on **acceptable use agreement** (appendix 1)
- Working with the DSL and/or **prevent lead** to ensure that any online safety incidents are logged (seeappendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College's **behaviour policy**

This list is not intended to be exhaustive.

**Parents:** Parents are expected to:

- Notify a member of staff, Co-Principals of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on **acceptable use agreement** of theCollege's IT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations andwebsites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

**Visitors and members of the community:** Visitors and members of the community who use the College's IT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use agreement (appendix 2).

**Breadth of Online Safety Issues:** We classify the issues within online safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention togroom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

These issues are to be managed by reducing availability, Restricting access, promoting safe and responsibleuse.

**Acceptable use definition:** The widespread use and availability of technology and social networks presents opportunities and also risks. This guide sets out what practices are deemed acceptable and those that are unacceptable. It is not our intention to prevent anyone from using technology or social media, but merely to ensure that when they do use these technologies they do so in a manner that protects themselves, their peers, and the reputation of the College.

We accept that students regularly bring their own devices into College, and if used sensibly these can enhance the learning experience. You must, however, be guided by your class teacher about the appropriate use of tablets and laptops in class and respect and comply with their views. Although the College cannot control the use of social media offsite and out-of-hours, should any material come to light that is defamatory, abusive, or offensive, or involves bullying and contravenes the ethos and values of the College, we will take steps to investigate, and where necessary impose sanctions, suspensionsor exclusion. Our advice is simple: enjoy the benefits of technology and social media, but respect College policy, respect your peers, and think before you post or send material or images.

**Educating students about online safety:** Students will be taught about online safety as part of the curriculum:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.
The College will use assemblies to raise students' awareness of the dangers that can be encountered onlineand may also invite speakers to talk to students about this.

We recognise that peer-on-peer abuse can occur online and to this end we teach students how to spot early warning signs of potential abuse, and what to do if students are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physicallyand emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber-bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, eg involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Staff should be vigilant in lessons where students use the Internet. If staff allow the use of mobile devices intheir lessons, they must ensure that they are used in line with College policy.

**Educating parents about online safety:** The College will raise parents' awareness of internet safety in letters or other communications home, and via the SchoolBase notice board in information via our website portal. This policy will also be shared with parents. Online safety will also be covered during parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Co-Principals and/or the DSL and prevent lead. Concerns or queries about this policy can be raised with any member of staff or the Co-Principals..

**Cyber-bullying:**
**Definition:** Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the College's behaviour policy.)

**Preventing and addressing cyber-bullying:** To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The College will actively discuss cyber-bullying with students, explaining the reasons why it occurs, theforms it may take and what the consequences can be. Heads of Year and Personal Tutors will discuss cyber-bullying with their students and tutees, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber- bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, proprietors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail). The College also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College's **behaviour policy**. Where illegal, inappropriate or harmful material has been spread amongstudents, the College will use all reasonable endeavours to ensure the incident is contained. The DSL or prevent lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

**Examining electronic devices:** College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device,staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL,Prevent lead or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searchingand confiscation. Any complaints about searching for or deleting inappropriate images or files on students' electronic deviceswill be dealt with through the College's complaints procedure.
**Online Sexual Harassment:** Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviour and provide an environment that may lead to sexual violence. online sexual harassment includes: non-consensual

sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, are unacceptable and will dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (eitherin isolation or in connection with offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. They also include the potential for the impact of the incident to extend further than the College's local community (e.g. for images or content to be shared around neighbouring Colleges/Colleges) and for a victim (or alleged perpetrator) to become marginalised andexcluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

a. The UK Safer Internet Centre, which provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. Providing expert advice and support for College staff with regard to online safety issues and when an allegation is received.
b. If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

**IT-Based Sexual Abuse (Including Sexting):** The impact on a child of IT-based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. IT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there

needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobiletelephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the College and may constitute a criminal offence. The College will treat incidences of sexting (both sending and receiving) as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of students is illegal. This will lead to criminal investigation and the individual being barred from working with students, if proven. Adults should not use equipment belonging to the College to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability ofthe adult to continue to work with students. Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of students or other unsuitable material arefound, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

**Technology and Prevent Duty:** As part of an integrated policy linked to the Prevent strategy, the College also has a duty to ensure that students are prevented and protected from the risk of being radicalised through the access to extremist propaganda, e.g. from ISIL. The College must promote British values through the curriculum and SMSC and SRE. Teachers must also be aware of their responsibility to monitor and report any serious concerns they have about a student's use or access to inappropriate material, especially that which undermines British values and tolerance of others. The College's network and facilities must NOT be used for the following activities:

- Accessing or downloading pornographic material
- Gambling
- Accessing sites or social media channels that promote extreme viewpoints and radical propaganda
- Gambling
- Soliciting for personal gain/profit
- Revealing or sharing proprietary or confidential material
- Representing personal opinions about the College
- Positing indecent or humiliating images or remarks/proposals

**Assessing Risks Online:** We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the College network. The College cannot accept liability for any material accessed, or any consequences of Internet access.

Developing technologies, such as mobile phones with Internet access are not governed by the College's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our students in Boarding, who could have unsupervised access to the internet when using their own devices in their free time. To address this, the College works with students across our age range to ensure that students are educated clearly about the risks of both social media and internet use, alongside regularly monitoring of device usage as appropriate.

- We will audit IT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Governance Advisory Board will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in College is allowed.
- Any person not directly employed by the College will not be provided with access to any of the College systems with the exception of filtered *Wi-Fi* access.
- David Game College takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- The College recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, wewill supplement the systems filtering with behaviour management and additional staff/student training.

**Phishing and PharmingDefinition**: A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic looking, albeit fake, web page. The target is asked to input information like a username and password, or even additional financial or personal data.
The miscreant that orchestrates the phishing scheme is able to capture this information and use it to further criminal activity, like theft from a financial account and similar types of criminal activity.
The College has no intention of changing its financial information, therefore never accept an email with a link pretending to be the College's accounts department.
Top tips:

- Never click on hyperlinks in email from an unknown sender, rather manually type the URL into the web browser itself
- Never enter sensitive information in a pop-up window except at those sites that an individual knows to be trustworthy
- Verify HTTPS on the address bar - whenever a person is conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S"confirms that the date is being conveyed through a legitimate, secured channel
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers
- Education on phishing and pharming attacks - staying abreast of phishing scams and the technology and techniques designed to prevent them is crucial. A plethora of reliable educational resources exist on the Internet that are designed to assist a person in preventing phishing attacks
- Report phishing and pharming to the financial institution, the FTC, and the Internet Crime Complaint Center

**Characteristics of a strong password**

- At least 8 characters – the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ? ]

**Note:** do not use < or > in your password, as both can cause problems in web browsers
A strong password is hard to guess, but it should be easy for you to remember – a password that has to bewritten down is not strong, no matter how many of the above characteristics are employed.

**Protecting Personal Data:** Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018. The College recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The College will act responsible to ensure we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

**Acceptable use of the internet in the College:** All students, parents, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of the College's IT systems and the internet (appendices 1 and 2). Visitors will be expectedto read and agree to the College's terms on acceptable use if relevant. Use of the College's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, proprietors and visitors (where relevant) toensure they comply with the above.
More information is set out in the **acceptable use agreements** in appendices 1 and 2.

**Do's and Don'ts**

**DO:**

1. Talk with your parents about your use of social media and before you open accounts on Facebook and Twitter, Instagram and Snapchat
2. Keep your phone on silent or preferably switch it off during lessons
3. Consider carefully how you present yourself on Facebook and only refer to your own views and notothers' (unless you have their full consent)
4. Think carefully about posts that you make and how they may be interpreted. It is important that youdo not offend people, use abusive language or discriminate against anyone
5. Keep your language civil and polite; do not use profanities when communicating
6. Keep details of your personal life and relationships private
7. Talk to members of staff if you have concerns about using social networks or if you have a suspicionabout a contact
8. Report to your parents and/or a member of staff any incident of cyberbullying or intimidation/humiliation
9. Make sure you understand how to enable privacy settings. Remember that material posted cannotalways be easily removed, so take great care in what you write about yourself and especially others
10. Remember that jokes can be misinterpreted or considered offensive and that you must respect thesensitivities of others

**DO NOT:**

1. Give anyone your user name or password for the College network
2. Play music using MP3 players during lessons or in the corridors
3. Play music from your phone or portable device that may annoy or distract others
4. Access social media or emails during lessons; this can be done during lunch time and in the canteen
5. Try and contact any member of staff by phone, personal email or through social media channels. Staff can contact you via the approved College SMS system or through the designated emails viathe College network
6. Try and access material or images from extremist groups as these are closely monitored and the College has a legal duty to prevent students from being at risk of radicalisation

7. Try and attempt to access inappropriate material, such as pornography, extreme sites or those sites that undermine British values; the College will filter such sites and a monitoring software will be putin place
8. Access gaming or gambling sites while at College
9. Cut and paste material from the web and claim it as your own work – this is plagiarism and this is taken very seriously by the College and the examination boards. You can cite, through appropriate referencing, an article or use of quote and staff can guide you in this area. You must respect the law of copyright and intellectual property of others
10. Create and display or disseminate offensive material, which includes, but is not limited to, racism, pornography, sexism, bullying (including homophobic bullying), blasphemy, or defamatory material.
11. Do not bring the College into disrepute through your communication via emails, your phone, oracross social media channels.
12. Attempt to "hack" into the network of the College or have any unauthorised access to any part of thenetwork; this is considered a serious breach of our online safety policy.
13. Attempt to destroy work files or alter College computer terminals or software in any way.
14. Use phones or other portable devices to record (visually or auditory) another student or a member ofstaff; this will be considered a very serious breach of privacy and will have significant sanction attached to it
15. Try and contact teachers or any member of staff through social media; do not ask them to link with you as this is unacceptable and prohibited
16. Talk about or discuss members of staff or teachers on your social networks as this could lead to sanctions being taken against you
17. Take an image/photograph of another student or member of staff using a smart phone or tablet device unless you have express permission; this is unlikely to be granted by staff for reasons of professional conduct. You must ask friends before tagging them in photos.
18. Share any image of a person without their permission
19. Impersonate any other person or use another person's account without their full permission
20. Post anything that may seem insulting, intimidating, threatening or abusive. The College has arobust anti-cyber bullying policy and this will be enforced if a student is found to have conducted in some form of cyber bullying. Sex-texting will not be tolerated by the College.
21. Comment on College policy using social networks - if you need to discuss this, please raise it with the relevant person/appropriate channels. You will been given an opportunity to articulate your comments at a meeting or during the Student Council meetings.

**Students using mobile devices in the College:** Students may bring mobile devices into the College, but are not permitted to use them during:

- Lessons
- Personal Tutor time
- Clubs, sessions on the premises, or any other activities organised by the College

Any use of mobile devices in the College by students must be in line with the **acceptable use agreement** (see appendix 1). Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with theCollege's **behaviour policy**, which may result in the confiscation of their device.

**Staff using work devices outside the College:** Staff members using a work device outside the College must not instal any unauthorised software on the device and must not use the device in any way which would violate the College's terms of acceptable use agreement, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected with a strong password, so too their online login details to CollegeBase, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside the College. Any USB devices containing data relating to the College must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the IT manager. Work devices must be used solely for work activities.

**How the College will respond to issues of misuse:** Where a student misuses the College's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the College's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The College will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**Sanctions and Enforcement:** If a member of the College community breaches any of the terms set out in our policy and guidance documents, sanctions can be applied and in serious cases, any offender will be reported to the appropriate authority. This will be exercised as a case-by-case basis and proportionately. Both staff and students will be subject to disciplinary action depending on the action they have taken and its impact on others, the reputation of the College or in terms of undermining British values.

**Specifics**: Members of the College community cannot:

1. Disclose their password and user name to other people
2. Read another person's email without consent
3. Take photographs of other students without their permission
4. Post or share images of other members of the College community without their full permission; youmust delete certain images if requested by a member of staff
5. The College computers cannot be used for gamming or gambling
6. If there has been an accidental download of material that is inappropriate, a member of staff must be informed immediately
7. Use social media during College time
8. Mobile phones must be switched off or placed on silence during lessons and key extracurricular activities e.g. assemblies and events
9. Knowingly obtain unauthorised access to any part of our network or system through hacking; this isa criminal offence
10. You must respect copyright laws and understand that you cannot copy and paste other people work and claim it as your own - this is plagiarism
11. Display or distribute/share offensive material, which includes, but is not limited to: racism, sexism, pornography, bullying, homophobic bullying or negative comments, defamation, or images that are likely to offend others. Anyone found to have offensive material will be subject to seriously disciplinary proceedings, which may result in suspension, exclusion and in serious cases involvement of the police or relevant authorities
12. Share or distribute any material that is likely to undermine British values and could radicalise others
13. The College has the right to confiscate and investigate the content of e-equipment if has seriousground that an offence has occurred and the Police may become involved for legal reasons
14. Students must treat all IT equipment with respect and not print out lengthy items and use upsignificant amounts of paper
15. The College does allow students to being in their own devices, but they are not allowed to physicallyconnect with the College system unless they have the permission from the IT manager
16. Mobile phone communication between staff and students is permissible during visits and field trips,but this will usually be on a College dedicated mobile
17. Students cannot film or record other students or their teacher during class or outside of class unlesswith the specific permission, which for staff will normally be in writing.
18. Mobiles cannot be taken into the science laboratories and must be left in the prep room
19. Mobiles must be switched off and handed to an invigilator for safe keeping when this request isissued prior to the announcement of a formal examination
20. Mobiles must be switched off during lessons and mocks and not be left on the tables or desks
21. Members of the College community cannot communicate through personal emails or via socialmedia channels inside or outside of College. Communication is acceptable via official SMS andemail systems
22. If the Co-Principals have reasonable grounds to suspect that inappropriate communication has occurred between staff and students, then mobiles or other devices may be secured for examination.

**Training:** All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including **cyber-bullying** and the risks of **online radicalisation**. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). The DSL, deputy and prevent lead will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subjectof online safety at regular intervals, and at least annually. Proprietors will receive training on safe internet use and online safeguarding issues as part of theirsafeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy as wellas the prevent policy**.**

**Remote Learning: (Please see our Remote Learning Policy for more details):** Where there are periods in which the College is forced to close, yet continue to provide education (such as during the COVID-19 Pandemic) it is important that David Game College supports staff, students and parents to access learning safely, especially considering the safety of our vulnerable students. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the College recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns, and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the College's staff and students respective Behaviour - Code of Conducts. Additionally, College name will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The College will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programmes the College is expecting students to use andhow to access these alongside how students and parents can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our Colleges Remote Learning Policy.

Additionally, the Co-Principals has a duty of care for ensuring the safety (including online safety) of members of the College community, with the day to day responsibility being delegated to the Online Safety Lead who is our DSL. The Co-Principals and the DSL are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their College-issued IT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the College's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

**Monitoring arrangements:** The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can befound in Appendix 4.

**Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Prevent policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

**Appendix 1: acceptable use agreement (students and parents/guardians/carers)**

**Acceptable use of the College ICT systems and internet: agreement for students andparents/guardians/carers**

Name of student:

When using the College's IT systems and accessing the internet in the College, I will not:

- **Use them for a non-educational purpose**
- **Use them without a teacher being present, or without a teacher's permission**
- **Access any inappropriate websites**
- **Access social networking sites (unless my teacher has expressly allowed this as part of alearning activity)**
- **Use chat rooms**
- **Open any attachments in emails, or follow any links in emails, without first checking with a teacher**
- **Use any inappropriate language when communicating online, including in emails**
- **Share my password with others or log in to the College's network using someone else'sdetails**
- **Give my personal information (including my name, address or telephone number) toanyone without the permission of my teacher or parent/guardian/carer**
- **Arrange to meet anyone offline without first consulting my parent/guardian/carer, orwithout adult supervision**
- **If I bring a personal mobile phone or other personal electronic device into the College:**
- **I will not use it during lessons, tutor group time, clubs or other activities organised by theCollege, without a teacher's permission**
- **I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online**
- **I agree that the College will monitor the websites I visit.**
- **I will immediately let a teacher or other member of staff know if I find any material which mightupset, distress or harm me or others.**
- **I will always use the College's IT systems and internet responsibly.**

| | |
|---|---|
| Signed (student): | **Date:** |

**Parent/carer agreement:** ***I agree that my child can use the College's IT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for students using the College's IT systems and internet, and for using personal electronic devicesin the College, and will make sure my child understands these.***

| | |
|---|---|
| **Signed (parent/carer):** | **Date:** |

**Appendix 2: acceptable use agreement** (staff, proprietors, volunteers and visitors)

## Acceptable use of the College’s IT systems and the internet: agreement for staff, proprietors, volunteers and visitors

Name of staff member/proprietor/volunteer/visitor:

- **When using the College’s IT systems and accessing the internet in the College, or outside theCollege on a work device, I will not:**
- **Access, or attempt to access inappropriate material, including but not limited to materialof a violent, criminal or pornographic nature**
- **Use them in any way which could harm the College’s reputation**
- **Access social networking sites or chat rooms**
- **Use any improper language when communicating online, including in emails or othermessaging service**
- **Install any unauthorised software**
- **Share my password with others or log in to the College’s network using someone else’sdetails**

**I will only use the College’s IT systems and access the internet in College, or outside College ona work device, for educational purposes or for the purpose of fulfilling the duties of my role.**

**I agree that the College will monitor the websites I visit.**

**I will take all reasonable steps to ensure that work devices are secure and password-protectedwhen using them outside College, and keep all data securely stored in accordance with this policy and the College’s data protection policy.**

**I will let the designated safeguarding lead (DSL) and IT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will alsodo so if I encounter any such material.**

**I will always use the College’s IT systems and internet responsibly, and ensure that students inmy care do so too.**

| | |
|---|---|
| **Signed (staff member/proprietor/volunteer/visitor):** | **Date:** |

**Appendix 3 – Use of photographs of students and data protection form (to be completed by all newparents)**

**Photographs**

David Game College would like your permission to use photographs of your child for marketing and publicity purposes including our website, prospectus, adverts, press releases and other marketing literature such as brochures and leaflets. We will not use names next to photographs of students on the website (in accordance with the DfE guidelines).

Parent/Guardian's name: ____________________________________________________________

Student's name: ________________________________________________________________

Student's year group/form: ________________________________________________________

Please tick the appropriate box.

I give my permission for David Game College to use photographs of my child for marketing and publicitypurposes □

I do not give my permission for David Game College to use photographs of my child for marketing andpublicity purposes □

Signature:…………………………………………………………………………… Date……………………………………………….

Please print name:……………………………………………………………

**Data Protection Statement**

Information about parents/carers is collated, stored and used by David Game College for the purposes of keeping you informed of events and activities concerning David Game College and for fundraising. By signing this form, you consent to David Game College using your data in this way. This information will not be used for any other purpose or passed to any person outside the College without your consent.

I consent to David Game College using my data for the stated purposes □

I do not consent to David Game College using my data for the stated purposes □

Signature:…………………………………………………………………………… Date……………………………………………….

Please print name:……………………………………………………………

**Appendix 4 - Acceptable Use of Mobile Phones and 3G/4G/5G compatible devices**

**Purpose:** It is our intention to provide within this policy an environment in which children, parents, and staff are safe from images being recorded and inappropriately used, in turn eliminating the potential use to interfere withthe dignity and privacy of all individuals and thus compromise the confidentiality of the children in our care.

The widespread ownership of Mobile phones and 3G/4G/5G compatible devices (referred to throughout this document as mobile devices) among young people requires that College administrators, teachers, students, parents and carers take steps to ensure that these devices are used safely and responsibly at College. This Acceptable Use Policy is designed to ensure that potential issues involving mobile devicescan be clearly identified and addressed, ensuring the benefits that they can provide can continue to be enjoyed by our students.

The College has established the following Acceptable Use Policy for mobile devices that provides teachers, students, parents and carers guidelines and instructions for the appropriate use of these devices during the time students are under the care of the College, inclusive of the academic day, theboarding program, on campus and all educational visits.
Students, their parents or carers must read and understand the Acceptable Use Policy as a conditionupon which permission is given to bring mobile devices to College.

**Rationale:**

- The College recognises that personal communication through mobile devices such as mobile technologies is an accepted part of everyday life, therefore such technologies are to be used responsibly and in accordance to the Acceptable Use Policy.
- David Game College accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about commuting long distances to College. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently.

**Responsibility:**

- It is the responsibility of students who bring mobile devices to College to follow the guidelines outlined inthis document.
- The decision to provide any mobile devices to their children should be made by parents or carers. It is important that parents understand the capabilities of these devices and the potential uses or misuses of those capabilities. If needed, guidance to this information can be signposted by the College.
- Parents/carers should be aware that if their child brings any device, including a mobile phone to College,the College does not accept responsibility for any loss, damage or costs.
- Parents/carers are reminded that in cases of emergency, the College remains a vital and appropriate point of contact and can ensure your child is reached in a relevant and appropriate way. Parents/carers are requested that in cases of emergency they contact the College first so we are aware of any potential issue and may make any necessary arrangements.

**Acceptable Uses:**

- Mobile phones should be switched off and kept out of sight during classroom lessons in order to minimize disruption or distraction.
- Mobile phones should not be used in any manner or place that could be disruptive to the normal routineof the College.
- The College recognizes the importance of emerging technologies present in modern mobile devices e.g. phones, camera and video recording, internet access, MP3 and MP4 playback, blogging, etc. Teachers may wish to utilise these functions to aid teaching and learning and students may have the opportunity touse their mobile phones or mobile devices in the classroom. On these occasions students may use their mobile phones in the classroom when express permission has been given by the teacher. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.
- Headphones/earphones should only be used during private study or travelling to and from College with permission from the teacher.

**Unacceptable Uses:**

- In order to protect one’s privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, surf the internet, take photos or use any other application during College lessons, other educational activities such as assemblies, or in the Dining Hall.

- Mobile devices should not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times in order to respect the learning environment. Using mobile phones to bullyand threaten other students is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to the Anti-bullying and Online Safety Policies.)
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may causeembarrassment or discomfort to their fellow students, staff or visitors to the College.
- Disruption to lessons caused by a mobile phone or any mobile device may lead to disciplinaryconsequences.
- Safeguarding, privacy and respect are paramount at David Game College. To this end, it is prohibited to take a picture of or record a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images and may be requested to turn over the deviceto the Co-Principals and/or the Designated Safeguarding Lead.
- Headphones/earphones should not be used whilst moving around campus during the College day, whilstwaiting for or during lessons and assemblies, or in the dining halls.

**Theft or damage:**

- Mobile phones or any mobile devices that are found in the College and whose owner cannot be locatedshould be handed to the front office reception.
- The College accepts no responsibility for replacing lost, stolen or damaged devices.
- The College accepts no responsibility for damage to or loss of mobile phones or mobile devices whiletravelling to and from College.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorized phone callscannot be made on their phones or other mobile devices. Students must keep their password/pin numbers confidential.

**Inappropriate conduct:**

- Under exam regulations, mobile phones are prohibited from all examinations. Students MUST give phones to invigilators before entering the exam hall. Any student found in possession of a mobile phoneduring an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.
- Any student who uses vulgar, derogatory, or obscene language while using a mobile phone may facedisciplinary action.
- In order to ensure all boarders study time is respected, boarding students MUST not use their mobile phones or mobile devices during evening study hall hours unless explicitly required by their teacher for aspecific assignment.
- The College values the health and wellbeing of every student. To this end, boarding students MUST not use their mobile phones or mobile devices after evening checks are made in the Houses or after evening"lights out".
- Students with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using messages, taking/sending photos or objectionable images, and phone calls. Students using mobile phones to bully other students will face disciplinary action. (It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the College may consider it appropriate to involve the police).
- Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence, and the College is obligedto report any findings of this nature to the police and local authority.
- Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence, whichobliges the College to report to the police and local authority.

**Measures:** The following measures may be used in consultation and conjunction with the Anti-bullying, Child Protection and Safeguarding, E-Safety and IT Policies. The Online Safety Coordinator (DSL) must beconsulted when inappropriate conduct requires a mobile phone to be confiscated and searched.

- Students who violate the rules set out in this document could face having their phones and/or mobile devices held by teachers, House Parents, Deputy House Parents or House Tutors until the end of the class period or study session. If the device is being used inappropriately the student must give it to thesupervising adult if requested.
- Violation of the rules set out in this document are subject to the disciplinary measures set out in the Behaviour

Management Policy, which can be found on the policy section of the College’s Website.

I have read and understand this policy:

Student Signature:……………………………………………………………………………. Date………………………………………………….

Please print name:…………………………………………………………………………….

Parents: Informed via email communication

## Appendix 5: online safety training needs – self-audit for staff

| | |
|---|---|
| Online safety training needs audit | |
| Name of staff member/volunteer: | **Date:** |
| **Do you know the name of the person who has lead responsibility foronline safety in the College?** | |
| **Do you know what you must do if a student approaches you with a concern or issue?** | |
| **Are you familiar with the College's acceptable use agreement for staff, volunteers, proprietors and visitors?** | |
| **Are you familiar with the College's acceptable use agreement for students and parents?** | |
| **Do you regularly change your password for accessing the College'sIT systems and use a strong password?** | |
| **Are you familiar with the College's approach to tackling cyber-bullying?** | |
| **Are there any areas of online safety in which you would like training/further training?**<br>**Please record them here.** | |

**Appendix 6: online safety incident report log**

Also see the NSPCC **What to do if a student or a teacher reports an online safety incident** flowchart.

**Online safety incident report log**

| Date | Where the incident took place | Description of the incident | Action taken | Name and signature of staffmember recording the incident |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |