e-safety ICT policy

Last reviewed: Alexandra Raen & John Dalton [June 2018]

Next review due by: June 2019

Aims

David Game College aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, proprietors and 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 pupils. It comes under the umbrella of Safeguarding and also includes the requirements of the Prevent Strategy, promoting British values and prevents pupils from becoming radicalised by exposure and access to extremist propaganda. 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 pupils 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 the acceptable use of technology.

The following is a list of possible risks pupils 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 who 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 pupils
- 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

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for colleges on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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 Safeguard Children (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 e 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, and the Internet while at the College.

Roles and responsibilities

The Proncipal and Vice Principals, working in conjunction with our ICT managers, are responsible for ensuring the e-safety of the College community. Our Head of ICT will take operational responsibility for e-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 of the College community and that appropriate steps should be taken if an incident occurs. The Leadership Team will also review e-safety and the acceptable use of technology in the College during their regular meetings.

The Head of ICT will act as the e-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 pupils should be on a professional level and only carried out using official communications systems. In addition, e-safety must be embedded in all aspects of the curriculum and other school activities. Students should have read, understood and signed the guidance notes on e-safety. Parents will be copied on student guidance notes.

Our Head of ICT is also the network manager and he has a specific duty of care to ensure that suitable control and filters are in place and that the system is secured and risk-assessed based on College policies.

In particular, the ICT Head should ensure that:

- All users have clearly defined access rights to the school ICT systems
- Servers, wireless systems and cabling are securely located and physically protected and have access 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 school site unless safely encrypted
- All users are provided with a user name and password
- Regular reviews of the network system are taken to examine vulnerabilities and risks • An agreed policy is in place regarding the use of removal media – memory sticks, CDs, DVDs
- 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 pupils prior permission (written)
- Staff and pupils 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 pupils inside or outside college unless they are using the designated college system and that all communications are subject to inspection and review
- The use of social networking sites within the College is only allowed in appropriately controlled situations and support of legitimate curriculum activities
- Students and staff must report any inappropriate material about them or others online which could bring the College into disrepute

The proprietor

The proprietor at David Game College, the Senior Team, has overall responsibility for monitoring this policy and holding the principal and vice principals 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 proprietor who oversees online safety on behalf of the Senior Team, John Dalton (johndaltonlsp@gmail.com)

All proprietors, 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) of the College's ICT systems and the internet (see appendix 2)

The principal

The principal and vice-principals 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, rachelsherman@davidgame-group.com as well as potentially our **designated prevent lead**, John Dalton (johndaltonlsp@gmail.com), are set out in our **child protection and safeguarding policy** also our **prevent policy**.

The DSL takes lead responsibility for online safety in College, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the college
- Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line 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 on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to the principal and/or vice-principals

This list is not intended to be exhaustive.

The ICT manager

The ICT 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 basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT 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 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.

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 ICT systems and the internet (appendix 2), and ensuring that pupils 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 (see appendix 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, principal or vice-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 the College's ICT systems and internet (appendix 1)

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

- 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 ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on **acceptable use agreement** (appendix 2).

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, suspensions or 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 pupils about online safety

Pupils 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 pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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 principal and/or the DSL and prevent lead.

Concerns or queries about this policy can be raised with any member of staff or the principal or vice-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 pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Head of Years and Personal Tutors will discuss cyber-bullying with their pupils 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 pupils, 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 among pupils, 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 pupils' 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 pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the College's complaints procedure.

Sexting

Definition

Sexting is when someone has received or sent explicit images, videos or messages. (See also the College's behaviour policy.) Sex-texting is now common amongst teenagers and the College is clear in its view that any student who sends a text that humiliates or offends another student will be disciplined and may be suspended. The College has a duty of care to ensure that students cannot access materials that may harm them or put them at risk. Filters will be put in place to block pornographic material, access to gaming and gambling sites and other restricted sites. This will be regularly reviewed.

All staff members and volunteers should be aware of the dangers and signs of sexting. If they have any concerns or become aware of young people sharing explicit images or videos of themselves or others should follow the guidance as set out by the NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/sexting-advice-professionals/

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:

- Assessing 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 school
- Positing indecent or humiliating images or remarks/proposals

Phishing and Pharming

Definition

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 including a training course here
- 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 be written down is not strong, no matter how many of the above characteristics are employed.

Acceptable use of the internet in the College

All pupils, parents, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of the College's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to 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 pupils, staff, volunteers, proprietors and visitors (where relevant) to ensure 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 not others' (unless you have their full consent)
4. Think carefully about posts that you make and how they may be interpreted. It is important that you do 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 suspicion about 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 cannot always 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 the sensitivities 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 via the 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 put in 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, or across social media channels.
12. Attempt to "hack" into the network of the college or have any unauthorised access to any part of the network; this is considered a serious breach of our e-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 of staff; 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 a robust 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 school 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

Pupils using mobile devices in the College

Pupils may bring mobile devices into the College, but are not permitted to use them during:

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

Any use of mobile devices in the College by pupils must be in line with the **acceptable use agreement** (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the College'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 install 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 SchoolBase, 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 of 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 ICT manager.

Work devices must be used solely for work activities.

How the College will respond to issues of misuse

Where a pupil misuses the College's ICT 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 ICT 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 must 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. You should not post or share images of other members of the College community without their full permission; you must 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. Students and staff cannot 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. You must not knowingly obtain unauthorised access to any part of our network or system through hacking; this is a 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. You cannot 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. You cannot 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 serious ground that an offence has occurred and the Police may become involved for legal reasons
14. Students must treat all ICT equipment with respect and not print out lengthy items and use up significant amounts of paper
15. The College does allow students to being in their own devices, but they are not allowed to physically connect with the College system unless they have the permission from the ICT 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 unless with 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 is issued prior to the announcement of a formal examination
20. Mobiles must be switched off during lessons and mocks and not on the tables or desks
21. Members of the College community cannot communicate through personal emails or via social media channels inside or outside of College. Communication is acceptable via official SMS and email systems
22. If the Principal or Vice 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 subject of online safety at regular intervals, and at least annually.

Proprietors will receive training on safe internet use and online safeguarding issues as part of their safeguarding 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 well as the prevent policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the DSL and prevent lead. At every review, the policy will be shared with the principal and proprietors.

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 (pupils and parents/guardians/carers)

.

Acceptable use of the College's ICT systems and internet: agreement for pupils and parents/guardians/carers	
Name of pupil:	
When using College's ICT 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 a learning 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's details** • **Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/guardian/carer** • **Arrange to meet anyone offline without first consulting my parent/guardian/carer, or without 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 the College, 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 might upset, distress or harm me or others.** **I will always use the College's ICT systems and internet responsibly.**	
Signed (pupil):	**Date:**
Parent/carer agreement: **I agree that my child can use the College's ICT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for pupils using the College's ICT systems and internet, and for using personal electronic devices in 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 ICT systems and the internet: agreement for staff, proprietors, volunteers and visitors	
Name of staff member/proprietor/volunteer/visitor:	
When using the College's ICT systems and accessing the internet in the College, or outside the College on a work device, I will not: • **Access, or attempt to access inappropriate material, including but not limited to material of 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 other messaging services** • **Install any unauthorised software** • **Share my password with others or log in to the College's network using someone else's details**	
I will only use the College's ICT systems and access the internet in College, or outside College on a 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-protected when 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 ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.** **I will always use the College's ICT systems and internet responsibly, and ensure that pupils in my care do so too.**	
Signed (staff member/proprietor/volunteer/visitor):	**Date:**

Appendix 3: 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 for online safety in the College?	
Do you know what you must do if a pupil 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 pupils and parents?	
Do you regularly change your password for accessing the College's ICT 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? Please record them here.	

Appendix 4: online safety incident report log

Also see the NSPCC **What to do if a pupil or a teacher reports an e-safety incident** flowchart.

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**