The Duke of York's Royal Military School

IT and Online Acceptable Use Policy

Date of Approval by Chairman on behalf of the Governing Body:	17/05/2022
Signed: Colonel A Thorne	
Position: Chairman	

Reviewed and agreed by the Board of Trustees.

Last reviewed:	May 2022
Next review by:	May 2023

ETHOS AND BOARDING AIMS

Ethos

Our aim is to provide all-round education with an academic focus. We will promote the full development of students by providing a secure, professional, and caring environment in which each student is encouraged to reach his or her individual potential and is prepared for the opportunities, responsibilities, and experiences of adulthood. These goals will be achieved in the context of a learning, spiritual, moral, and pastoral ethos, which respects values of Christian and other faith communities, and our unique military tradition.

Boarding Aims

- To promote the personal student values of courage, discipline, respect, integrity, loyalty, and commitment within an environment where learning is at its heart.
- To promote a pastoral environment in which **all** students can live, grow and be happy.
- To develop a sense of community and belonging within our 100% co-educational boarding school.
- To develop and foster supportive relationships between students, parents, staff, and other stakeholders.
- To understand and provide for the particular and evolving educational and boarding needs of the military community.
- To promote a respect for the rights of others and their property.
- To promote good manners and develop social skills.
- To promote the "student voice" in the discussion of boarding matters.
- To promote and develop the unique military ethos of the School.
- To provide a boarding environment which develops respect for others and where bullying or other forms of harassment are not tolerated.
- To provide students with a range of activities and experiences which will develop their character, resilience, and leadership skills, allowing students to make a positive contribution to our School community and beyond.
- To provide the highest quality boarding accommodation, pastoral care and medical care that complies with the National Minimum Standards for Boarding Schools and exceed them wherever possible.

CONTENTS

1. Introduction and Aims
2. Relevant Legislation and Guidance
3. Definitions
4. Unacceptable Use
5. Staff (including trustees, volunteers and contractors)
6. Students
7. Parents
8. Data Security
9. Protection from Cyber Attacks
10. Internet Access
11. Monitoring and Review
12. Related Policies

Appendix 1 - Social Media Cheat Sheet for Staff
Appendix 2 - Acceptable Use of the School's ICT Facilities and the Internet – Agreement for Students, Parents and Carers
Appendix 3 - Acceptable Use of the School's ICT Facilities and the Internet - Agreement for Staff, Trustees, Volunteers and Visitors
Appendix 4 - Glossary of Cyber Security Terminology
Appendix 5 - Actioning Concerns Raised Online

1. Introduction and Aims

Information and Communications Technology (ICT) is an integral part of the way our school works, and is a critical resource for students, staff (including the Senior Leadership Team), trustees, volunteers, and visitors. It supports teaching and learning, pastoral, and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety, and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents, and trustees.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policy on data protection, online safety and safeguarding in line with Kent County Councils (KCC) Online safety policy. It also takes into account the DFE statutory guidance Keeping Children Safe in Education (KCSIE), and the Kent Safeguarding Children Multi-Agency Partnership agreements.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching students safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including trustees, staff, students, volunteers, contractors and visitors.

Breaches of this policy will be dealt with in line with the school's Behaviour Policy, Staff Code of Conduct and Staff Disciplinary Policy and Procedure.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

"Users": anyone authorised by the school to use the ICT facilities, including trustees, staff, students, volunteers, contractors, and visitors.

"Personal use": any use or activity not directly related to the users' employment, study, or purpose.
"Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs. See Appendix 4 for a glossary of cyber security terminology.

4. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery).
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its students, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel.
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.
- Using websites or mechanisms to bypass the school's filtering mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal or members of SLT will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions to Unacceptable Use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion.

To be granted an exception, this would have to be agreed prior to the action being undertaken and should be requested in writing from the Principal or SLT with rational as to why. No action should be taken before an agreement is in place.

4.2 Sanctions

Students and/or staff who engage in any of the unacceptable activity listed above may face sanctions or disciplinary action in line with the school's policies on Behaviour, Staff Code of Conduct, Staff Disciplinary Policy, and Procedure.

5. Staff (including trustees, volunteers, and contractors)

5.1 Access to School ICT Facilities and Materials

The school's IT manager manages access to the school's ICT facilities and materials for school staff and students. This includes, but is not limited to:

- Computers, tablets, mobile phones, and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the SLT and IT manager. To access this information, you will need to submit your reason/rational for accessing this information via email to SLT and IT manager for approval.

5.2 Use of Phones and Email

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents and students and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the IT manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the school to conduct all work-related business.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.3 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The IT manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time or periods of work.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no students are present.
- Does not interfere with their jobs or prevent other staff or students from using the facilities for work or educational purposes.

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.6). Where breaches of this policy are found, disciplinary action may be taken.

Staff are not permitted to use their personal devices, such as mobile phones or tablets, for any form of recording or images of students. They must use registered work devices.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents could see them.

5.3.1 Personal Social Media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for social media accounts (see Appendix 1).

5.4 Remote Access

We allow staff to access the school's ICT facilities and materials remotely.

Our remote access is managed by the IT Manager. The access is through a cloud-based system using one drive and SharePoint.

If staff are using their own IT equipment to access these locations, then they must ensure that they are following the Data Protection policy. They must ensure that only the materials they use are pertinent to their role or required at that time.

If there is a concern over what has been downloaded the IT manager is able to monitor and report what has been downloaded and accessed by a staff member. This would be at the request and agreement of SLT.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the IT Manager and Data protection officer has stipulated.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

5.5 School Social Media Accounts

The school has official social media pages, managed by our Marketing department. Staff members who have not been authorised to manage, or post to, these accounts, must not access, or attempt to access these accounts.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.6 Monitoring of School Network and Use of ICT Facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.

Only authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures, and standards.
- Ensure effective school and ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

5.7 Engagement and Education of Staff

The IT and Online Acceptable Use policy will be discussed with staff as part of induction and will be reinforced and highlighted as part of safeguarding responsibilities.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential when using School systems and devices.

All members of staff should be aware that their online conduct out of School could have an impact on their role and reputation within School. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Members of staff with a responsibility for managing filtering systems or monitor IT use will be supervised by the Senior Leadership Team and will have clear procedures for reporting issues or concerns.

The School will highlight useful online tools which staff should use according to the age and ability of the students.

6. Students

Students must adhere to the rules regarding Acceptable Use of the School's ICT Facilities and Internet detailed in Appendix 2.

- All students are advised to be cautious about the information given by others on sites. This is because other people may not be who they claim to be.
- Students are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, school details, IM/email address and specific hobbies/interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are asked to report any incidents of online bullying to the school.
- Students should not meet anyone that they have met through the internet, unless accompanied by a trusted adult.

6.1 Access to IT Laptops

Students should use laptops which have been supplied to them via the school for all learning and working in the school and should be used in line with the school's Imagery Use policy.

6.2 Search and Deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation. Searches will be completed by a member of the safeguarding team, under the supervision of another member of the safeguarding or Senior Leadership Team.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the Police, if a student discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable Use of ICT and the Internet Outside of School

Cases of unacceptable use of ICT and the internet by students when not on school premises will be reviewed as required and sanctions will be applied in accordance with the school's Behaviour policy.

6.4 Education

- Online safety will be promoted and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.
- Students will be supported in reading and understanding the IT and Online Acceptable Use policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PSHEE, RSE and other relevant programmes of study, covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety education approaches.
- The school will reward positive use of technology by students.
- The school will implement peer education to develop online safety as appropriate to the needs of the students.

6.5 Engagement and Education of Children and Young People Considered to be Vulnerable

The school is aware that some students may be considered to be more vulnerable online due to a range of factors.

The school will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate (e.g., SENCo).

7. Parents

- Parents and carers are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Parents and carers are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, school details, IM/email address and specific hobbies/interests).
- Parents and carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Parents and carers are asked to report any incidents of online bullying to the school.
- The school advises parents and carers to locate PC's and laptops in a highly visible part of the home, which can be regularly monitored.

7.1 Access to ICT Facilities and Materials

Parents do not have access to the school's ICT facilities as a matter of course. However, parents working for, or with the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access or be permitted to use the school's facilities at the Principal's discretion. Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating With or About the School Online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Parents will be allowed to film and take images of their child during performances/sporting event, any image or video taken that includes other children outside of their family must not be shared online or on any social media account as other students may also be included in such material.

We ask parents to sign the agreement in Appendix 2.

8. Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will use a password manager to help them store their passwords securely. The IT manager will generate passwords for students using a password manager/generator and keep these in a secure location in case students lose or forget their passwords.

When you first use this password, you will be asked to update with a password that you will be able to use and remember. It is expected that you will update this accordingly and keep this to yourself as these accesses your own private data and information. Passwords should contain a minimum of eight characters.

8.2 Software Updates, Firewalls and Anti-Virus Software

All the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data Protection

All personal data must be processed and stored in line with data protection regulations and the school's Data Protection policy.

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998 and GDPR. For more information on how the School uses its data please refer to the school's Data Protection policy.

Full information regarding the school's approach to data protection and information governance can be found in the school's Data Protection policy.

8.4 Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files, and devices.

These access rights are managed by the IT manager.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Data manager and the IT manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the Principal.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT manager.

9. Protection from Cyber Attacks

Please see the glossary (Appendix 4) to help you understand cyber security terminology.

The school will:

- Work with trustees and the IT department to make sure cyber security is given the time and resources it needs to make the school secure.

- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:

    - Check the sender address in an email.
    - Respond to a request for bank details, personal information, or login details.
    - Verify requests for payments or changes to information.

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:

    - **'Proportionate'**: the school will verify this using a third-party audit annually, to objectively test that what security is in place is fit for purpose.
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe.
    - **Up to date:** with a system in place to monitor when the school needs to update its software.
    - **Regularly reviewed and tested**: to make sure the systems are fit for purpose and secure as they can be.

- Back up critical data and this is completed once a day and store these backups on internal and external systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the IT manager.
- Make sure staff:

    - Enable multi-factor authentication where applicable.
    - Store passwords securely and do not share these with others.

- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure.
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet Access

The school wireless internet connection is secure. In order to protect our students and staff, the school employs the use of a filtering system to prevent access to unsuitable areas of the internet and monitors online activity via SENSO.

We have separate levels of filtering and access for staff/students and visitors to the school to ensure a secure environment and safe learning practices.

If students/staff or visitors come across any unsafe sites or practices, then they are to report this to the IT manager. If this is a safeguarding concern this should be reported to the DSL/DDSL (see Appendix 5).

10.1 Students

- Student access to Wi-Fi on school issued devices is available across the site between set hours dependant on year group.
- Student access to BYOD Wi-Fi is available in the boarding houses between set hours dependant on year group.
- All Wi-Fi access is filtered and monitored via the school's filtering and monitoring system.
- Students can request access to the BYOD through the IT Department.
- Any concerns with online use will be monitored and actioned accordingly should there be belief of a child protection issue.
- Students are not permitted to access the internet outside of the school Wifi/internet. This means that no student should tether a dongle or mobile data point on a school device.

10.2 Staff

Wi-Fi access is filtered and monitored. Online activity is monitored via Senso. Any breaches will be investigated by Senior Leadership Team.

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10.3 Parents and Visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Principal.

The Principal will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g., as a volunteer).
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

11. Monitoring and Review

The Principal, SLT and the IT manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy is reviewed annually and approved by the Board of Trustees.

12. Related Policies

This policy should be read alongside the following school policies:

- Safeguarding and Child Protection
- Behaviour
- Staff Discipline
- Data Protection
- Imagery Use

Appendix 1: Social Media Cheat Sheet for Staff

Do not accept friend requests from students on social media

10 rules for school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Do not share anything publicly that you wouldn't be just as happy showing your students.
6. Do not use social media sites during school hours.
7. Do not make comments about your job, your colleagues, our school, or your students online – once it's out there, it's out there.
8. Do not associate yourself with the school on your profile (e.g., by setting it as your workplace, or by 'checking in' at a school event).
9. Do not link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
10. Consider uninstalling social media apps from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or students).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster.
- **Google your name** to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this.
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if…

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior

leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages.
- Notify a member of the Senior Leadership Team about what is happening.

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school.
    - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in.

- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way.
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to Facebook or the relevant social network and ask them to remove it.
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the Police.

Appendix 2: Acceptable Use of the School's ICT Facilities and Internet: Agreement for Students and Parents/Carers

Acceptable Use of the School's ICT Facilities and Internet: Agreement for Students and Parents/Carers

Name of student:

When using the School's IT facilities (including connecting my own device to the *Bring Your Own Device (BYOD)* Wi-Fi) I will follow the school rules to keep myself safe. I must not:

- Break school rules.
- Access inappropriate websites.
- Use inappropriate language when communicating online, including in emails.
- Share semi-nude or nude images, videos, or livestreams, even if I have the consent of the person or people in the photo.
- Bully other people.
- Access, create, or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raise safeguarding issues).
- Access or share material that infringes copyright, and do not claim the work of others as my own.
- Download any films, music, games, or any other file that I do not have a license for, this is illegal and subject to UK law.
- Share my password with others or log in to the school's network using someone else's details.
- Use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Attempt to circumvent the content filters or other security measures installed on the School's IT network and systems, nor attempt to access systems that I do not have permission to access.
- Attempt to connect to any other Wi-Fi except for the correct School Wi-Fi provided and as instructed,
- Use a personal mobile phone to 'hot spot' on school laptops or PCs.
- Attempt to install software on, or otherwise alter, School IT computers, laptops, network, and systems either online or via software.
- Use VPN software. I understand using this type of software can put myself and the School at risk, and will result in sanctions being applied.
- Use the School's IT computers, laptops, networks, and systems in a way that breaches the principles of online behaviour set out above.

I will:

- Respect the privacy of others. I will not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Take all reasonable steps to protect my account from being misused by selecting a suitable password.

Student Agreement: I understand that the school can monitor my online activity and use of the school's ICT facilities and systems. 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 school's ICT systems and internet responsibly. I understand that the school can award sanctions if I do certain unacceptable things online, even if I am not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I also agree to ensure that there is appropriate level of parental control to avoid my child to access inappropriate sites or material.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable Use of the School's ICT Facilities and the Internet: Agreement for Staff, Trustees, Volunteers and Visitors

Acceptable Use of the School's ICT Facilities and the Internet: Agreement for Staff, Trustees, Volunteers and Visitors	
Name of staff member/trustee/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school 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 (or create, share, link to or send such material). • Use them in any way which could harm the school'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 or connect unauthorised hardware or devices to the school's network. • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its students or staff, or other members of the community. • Access, modify or share data I am not authorised to access, modify or share. • Promote private businesses unless that business is directly related to the school.	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school'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 also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/trustee/volunteer/visitor):	**Date:**

Appendix 4: Glossary of Cyber Security Terminology

These key terms from the NCSC will help you to understand the common forms of cyber-attack and the measures the school will put in place.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks, or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services, and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems, and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Appendix 5 Actioning Concerns Raised Online

Responding to Concerns Regarding Youth Produced Sexual Imagery or "Sexting"

- The Duke of York's Royal Military School ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of sharing, possessing, and creating youth produced sexual imagery (known as "sexting").
- The School will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff, and parents/carers.
- The Duke of York's Royal Military School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If a member of the School is made aware of incidents involving creating youth produced sexual imagery, they will immediately notify the Designated Safeguarding Lead who will:

    - Store any devices securely.
    - Carry out a risk assessment in relation to the student(s) involved.
    - Consider the vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care and/or the Police (as needed/appropriate).
    - Put the necessary safeguards in place for students e.g., offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the School's Behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
    - Inform parents/carers about the incident and how it is being managed.

- School staff will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The School will not send, share, or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the School network or devices, then the School will take action to block access to all users and isolate the image.
- The School will take action regarding creating youth produced sexual imagery, regardless of the use of School equipment or personal equipment, both on and off the premises.
- The School will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Responding to Concerns Regarding Online Child Sexual Abuse and Exploitation

- The Duke of York's Royal Military School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The School will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff, and parents/carers.
- The School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Area Safeguarding Team and/or Kent Police.
- If the School is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed on to the relevant authorities by the DSL.

- If a member of the School is made aware of incidents involving online child sexual abuse of a child, then they will immediately notify the Designated Safeguarding Lead who will:

    - Store any devices involved securely.
    - Immediately inform Kent Police via 101 (using 999 if a child is at immediate risk).
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for student(s) e.g., offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the School is implementing best practice and the Senior Leadership Team will review and update any management procedures where necessary.

- Where appropriate the School will involve and empower students to report concerns regarding online child sexual abuse e.g., using the CEOP website.
- The School will take action regarding online child sexual abuse regardless of the use of School equipment or personal equipment, both on and off the School premises.
- The School will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If students at other schools are believed to have been targeted, then the School will seek support from the Area Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

Responding to Concerns Regarding Indecent Images of Children (IIOC)

- The Duke of York's Royal Military School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The School will take action regarding Indecent Images of Children (IIOC) regardless of the use of School equipment or personal equipment, both on and off the premises.
- The School will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Area Safeguarding Team and/or Kent Police.
- If a member of staff is made aware of Indecent Images of Children (IIOC) then they will immediately notify the School's Designated Safeguard Lead who will:

    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g., the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the School is made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet or that indecent images of children have been found on the School's electronic devices, then the School will:

    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the webpage addresses which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

- Inform the Police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the Police only.

- If the School is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the School, then the School will:

  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the School's Whistleblowing procedure.
  - Contact the Police regarding the images and quarantine any devices involved until Police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with School procedures and follow appropriate School policies regarding conduct.

Responding to Concerns Regarding Radicalisation and Extremism Online

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately, and action will be taken in line with the School's Safeguarding and Child Protection and Anti-Radicalisation policies.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing School policies. If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

Responding to Concerns Regarding Cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of The Duke of York's Royal Military School will not be tolerated. Further details are set out in the School policies regarding Student Anti-Bullying and Behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the School community affected by online bullying.
- If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Area Safeguarding Team and/or Kent Police.
- Students, staff, and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The School will take steps to identify the bully where possible and appropriate. This may include examining School system logs, identifying and interviewing possible witnesses, and contacting the service provider and the Police, if necessary.
- Students, staff, and parents/carers will be required to work with the School to support the approach to cyberbullying and the School's online safety ethos.
- Sanctions for those involved in online or cyberbullying may include:

  - Those involved being asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
  - Internet access may be suspended at School for the user for a period of time. Other sanctions may also be used in accordance with the School's Behaviour, Online Safety and Acceptable IT and Imagery Use policies.
  - Parent/carers of students involved in online bullying will be informed.
  - The Police will be contacted if a criminal offence is suspected.

Responding to Concerns Regarding Online Hate

- All incidents of online hate reported to the School will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant School policies and procedures.
- The Police will be contacted if a criminal offence is suspected. If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Area Safeguarding Team and/or Kent Police.