The Duke of York's
Royal Military School
1803

Acceptable IT and Imagery Use Policy

Date of Approval by Principal		16/06/2021
Signed:	Mr Alex Foreman	

Reviewed and agreed by SLT.

Last reviewed:	Dec 2018 Jul 2019 Oct 2020 May 2021
Next review:	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 "*Manners Maketh Dukies*".
- 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.

Scope

This policy applies to all members of the School community, including staff, students, and parents. In this policy 'staff' includes teaching and non-teaching staff, Governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, students' carers and those with parental responsibility.

Online Behaviour

As a member of the School community, you should follow these principles in all your online activities:

- Ensure that your online communications, and any content you share online is respectful of others.
- Do not 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).
- Respect the privacy of others. Do 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.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own. Do not download any films, music, games, or any other file that you do have a license for, this is illegal and subject to UK law.
- Do not 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.
- Staff should not use their personal email, or social media accounts to contact students or parents, and student and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the School's IT, Laptops, PCs, and Systems

Whenever you use the School's IT facilities (including connecting your own device to the *Bring Your Own Device (BYOD)* Wi-Fi) you should follow these principles:

- Only access School IT network and systems using your own username and password. **Do not share your username or password with anyone else**.
- Take all reasonable steps to protect your account from being misused by selecting a suitable password.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT network and systems, and do not attempt to access systems that you do not have permission to access.
- Do not attempt to connect to any other Wi-Fi except for the correct School Wi-Fi provided and as instructed, using personal mobile phones to 'hot spot' is not allowed on school laptops or PCs.
- Do not attempt to install software on, or otherwise alter, School IT computers, laptops, network, and systems either online or via software. **The use of VPN software is strictly prohibited;** using this type of software puts both yourself and the School at risk, and if found will be subject to disciplinary action.
- Do not use the School's IT computers, laptops, networks, and systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT network and systems, and that the School can view content accessed or sent via its network and systems.

Care of School Laptops and PCs

Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages immediately to the IT Services Department, there may be a charge if damage or loss that is considered non-accidental or avoidable. The School is unable to provide technical support to personal devices and remain the responsibility of the owner.

Passwords

Passwords protect the School's network and computer systems and are your responsibility. They should not be obvious (for example 'password,' '123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights. You may be required to change your password on a timely basis, this will be enforced by the School's IT Systems, and you will be notified if and when to do so.

Use of School Network and Systems

The provision of School email accounts, Wi-Fi and internet access is for official School business, administration, and education. Staff and students should keep their personal, family, and social lives separate from their School IT use and limit as far as possible, any personal use of these accounts. Again, please be aware of the School's rights to monitor and access web history and email use.

Use of Personal Devices or Accounts and Working Remotely

All official School business must be conducted on School systems, and it is not permissible to use personal email accounts for School business. Any use of personal devices for School or pastoral purposes, and any removal of personal data, or confidential information from School systems – by any means including email, printing, file transfer, cloud (encrypted) memory stick – must be registered and approved by the IT Services Department.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies and will be subject to network filtering and monitoring.

Monitoring and Access

Staff, parents, and students should be aware that the School computers, laptops, email and internet usage will be filtered and monitored for safeguarding, conduct and performance purposes, and computers, laptops, web history and School email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by students, whether such use is permitted, may be confiscated and examined under such circumstances. The School may require staff to conduct searches of their personal accounts or devices if they were used for School business in contravention of this policy.

Compliance with Related School Policies

Staff and students are to read and comply with the School's Online Safety Policy, as well as all other related policies.

Retention of Digital Data

Staff and students must be aware that all emails sent or received on School systems will be kept in archive whether or not deleted. Student email accounts are closed within three months of the student leaving the School. Staff accounts are removed in line with national guidance. Important information that is necessary to be kept should be held on the relevant personnel or student file, not kept in personal folders, archives or inboxes. Hence, it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with School policy on personal use) is retained in the right place or, where appliable, provided to the right colleague. This would ensure important information should never be lost because of the School's email deletion protocol.

If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact the ICT Manager.

Breach Reporting

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School, regardless of whether the personal data falls into third party hands. This would include:

- Loss of an unencrypted laptop, USB stick or a physical file containing personal data.
- Any external hacking of the School's systems, e.g., through the use of malware.
- Application of the wrong privacy settings to online systems.
- Misdirected post, fax, or email.
- Failing to bcc recipients of a mass email.
- Unsecure disposal.

The School must generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (i.e., within 72 hours, and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or students become aware of a suspected breach, they should immediately notify the Data Protection Officer (DPO).

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they happen, the worse effects are contained and mitigated. This requires the involvement and support of all staff and students. The School's primary interest and responsibility is in protecting potential victims. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy, but failure to report a breach will be a disciplinary offence.

Official Use of Images/Videos of Students by the School

All images taken by the School will be used in a manner respectful of the eight Data Protection Principles.

This means that images will be:

- Fairly and lawfully processed.
- Processed for limited, specifically stated purposes only.
- Used in a way that is adequate, relevant and not excessive.
- Accurate and up to date.
- Kept on file for no longer than is necessary.
- Processed in line with an individual's legal rights.
- Kept securely.
- Adequately protected if transferred to other countries.

The Bursar and the Designated Safeguarding Lead are responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the School. This includes the management and implementation of the School's Use of Cameras and Images Policy. The Designated Safeguarding Lead with responsibility for the use of cameras and images is **Andy Agar**.

Written permission from parents or carers will be obtained before images/videos of students are electronically published by the School.

Written parental consent will be sought to take and use photographs off-site for professional, marketing and training purposes. This may be in addition to parental permission sought for on-site images. Written consent from parents will be kept by the School where student images are used for publicity purposes (such as brochures or publications), until the image is no longer in use.

Parental permission will be sought at the point of admission.

Use of Cameras and Images within the School

A record of all consent details will be kept securely on student files and SIMS. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of, and the record will be updated accordingly.

Images will not be kept for longer than is to be considered necessary. The Designated Safeguarding Lead, in conjunction with the IT department, will ensure that all photographs are permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

All images will remain on site at all times, unless prior explicit consent has been given by the Designated Safeguarding Lead and the parent or carer of any student captured in any photograph. Should permission be given to take images off site, all relevant details are to be recorded, for example who, what, when and why and data will be kept securely (e.g., with appropriate encryption).

The Designated Safeguarding Lead reserves the right to view any images taken and/or to withdraw or modify a staff member's authorisation to take or make images at any time.

Any memory stick, CD or storage device containing images of student to be taken off-site for further work will be suitably encrypted and will be logged in and out by the Designated Safeguarding Lead and monitored to ensure it is returned within the expected time scale.

Images or videos that include students will be selected carefully when used online and will not provide material that could be reused.

The full name of students will not be used on the website in association with photographs.

The School will not include any personal addresses, email addresses or telephone or fax numbers on video, on the website, in a prospectus or in other printed publications.

The School will only use images of students who are suitably dressed.

A student's work will only be published with their permission or their parents' consent.

Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.

All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.

Only School owned equipment (e.g., a digital or video camera provided by the School) will be used by staff to capture images of students for official purposes. Use of personal cameras or image recording devices, i.e., mobile phones, by staff is prohibited at all times.

Any apps, websites or third-party companies used to share, host or access student images will be risk assessed prior to use. The School will ensure that images are held in accordance with GDPR and suitable child protection requirements are in place.

Careful consideration is given before involving young or vulnerable students when taking photographs or recordings as they may be unable to question why or how activities are taking place.

The School will discuss the use of images with students in an age appropriate way.

Images will not be taken of any student against their wishes. A student's right not to be photographed is to be respected.

Photography is not permitted in sensitive areas such as changing rooms, toilets, and swimming areas.

Photographs will be disposed of should they no longer be required. They will be returned to the parent or carer, deleted, and wiped or shredded as appropriate. Copies will not be taken of any images without relevant authority and consent from the Designated Safeguarding Lead and the parent/carer.

Use of Photographs/Videos by Parents/Carers

Parents/carers are permitted to take photographs or DVD footage of events for private use only.

Parents/carers are only permitted to take or make recording within designated areas of the School. Photography is not permitted in sensitive areas such as changing rooms, toilets, and swimming areas.

The opportunity for parents/carers to take photographs and make videos can be refused by the School on health and safety grounds or for reasons of safeguarding and child protection.

Parents and carers who are using photographic equipment must be mindful of others when making and taking images.

The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.

Parents may contact the Designated Safeguarding Lead to discuss any concerns regarding the use of images.

Use of Photographs/Videos by Student

The School will discuss and agree age-appropriate acceptable use rules with students regarding the appropriate use of cameras, such as places students cannot take the camera (e.g. unsupervised areas and toilets).

The use of non-School provided devices e.g., mobile phones or a student's own digital cameras, is covered in the School's Online Safety Policy.

All staff will be made aware of the acceptable use rules regarding student use of cameras and will ensure that students are appropriately supervised when taking images for School or curriculum use.

Members of staff will model positive behaviour to the students by encouraging them to ask permission before they take any photographs.

Photographs taken by students for official use will only be taken with parental consent and will be processed in accordance with GDPR.

Parents/carers will be made aware that students will be taking photographs or videos of other students and will be informed how these images will be managed by the School e.g., these will be for internal use by the School only and not shared online or via any website or social media tool.

Photographs taken by students for School use will be carefully controlled and will be checked before sharing online or via digital screens.

Still and video cameras provided for use by students, and the images themselves, will not be removed from the School.

Use of Images of Student by the Media

Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's (or other relevant media) requirements can be met. A written agreement will be sought between parents and carers and the press which will request that a pre-agreed and accepted amount of personal information (e.g., first names only) can be published along with images and videos.

The identity of any press representative will be verified, and access will only be permitted where the event is planned, and where press is to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.

Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the School is to be considered to have acted in good faith.

Use of Professional Photographers

Professional photographers who are engaged to record any events will work according to the terms of the School's Online Safety and Acceptable Internet Use policies.

Photographers will sign an agreement which ensures compliance with the Data Protection Act and that images will only be used for a specific purpose, subject to parental consent.

Photographers will not have unsupervised access to students.

Use of Closed-Circuit Television (CCTV)/Webcams

All areas which are covered by CCTV/Webcams will be well signposted, and notifications displayed so that individuals are advised before entering the vicinity.

Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will generally be a maximum of 30 days.

Regular auditing of any stored images will be undertaken by the Designated Safeguarding Lead or other member of staff as designated by the Senior Leadership Team or Principal.

If cameras record activities taking place on the premises which are of a criminal nature or give any cause for concern, then information will be referred to the appropriate agency.

CCTV cameras will be appropriately placed within the School.

Further information can be found in the School's CCTV Policy.

Should IT hardware be disposed of the necessary data destruction certificates will be obtained in line with GDPR regulations.

Breaches of this Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting access to School IT network and systems.

Staff or students who become aware of a breach of this or the Online Safety Policy or are concerned that a member of the School community is being harassed or harmed online, must report it to a relevant member of staff.

Annex A – CCTV Policy

Purpose

The purpose of this policy is to regulate the management and operation of the Closed-Circuit Television (CCTV) System at The Duke of York's Royal Military School. It also serves as a notice and a guide to data subjects (including students, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV system.

The System is administered and managed by the School, who act as the Data Controller. This policy will be subject to review from time to time and should be read with reference to the School's Data Protection Policy. For further guidance, please review the Information Commissioner's CCTV Code of Practice.

All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds.

The School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

1. Objectives of the System

i. To protect students, staff, volunteers, visitors, and members of the public regarding their personal safety.

ii. To protect the School buildings and equipment, and the personal property of students, staff, volunteers, visitors and members of the public.

iii. To support the Police and community in preventing and detecting crime and assist in the identification and apprehension of offenders.

iv. To monitor the security and integrity of the School site and deliveries and arrivals.

v. To monitor staff and contractors when carrying out work duties.

vi. To monitor and uphold discipline among students in line with the School rules which are available to parents and students on request.

2. Positioning

i. Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives.

ii. Adequate signage has been placed in prominent positions to inform staff and students that they are entering a monitored area, identifying the School as the Data Controller, and giving contact details for further information regarding the system.

Commented [A1]: Should we have this extension in our Policy?

iii. No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.

iv. No images of public spaces will be captured except to a limited extent at site entrances.

3. Maintenance

i. The CCTV System will be operational 24 hours a day, every day of the year.

ii. The System Manager will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.

iii. The System will be checked and (to the extent necessary) serviced no less than annually.

4. Supervision of the System

i. Staff authorised by the School to conduct routine supervision of the System may include day or night security and relevant staff on duty.

ii. Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

5. Storage of Data

i. The day-to-day management of images will be the responsibility of the Head of Security who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.

ii. Images will be stored for 2-4 weeks, and automatically over-written unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the Police or local authority.

Commented [A2]: How long do we keep them for?

iii. Where such data is retained, it will be retained in accordance with the Act and our Data Protection Policy. Information including the date, time, and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log.

6. Access to Images

i. Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

ii. Individuals also have the right to access personal data the School holds on them (please see the Data Protection Policy), including information held on the System, if it has been kept. The School will require specific details including at least time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

iii. The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:

  a) Where required to do so by the Principal, the Police or some relevant statutory authority;

  b) To make a report regarding suspected criminal behaviour;

c) To enable the Designated Safeguarding Lead or the appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;

d) To assist the School in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;

e) To data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out above;

f) To the School's insurance company where required to pursue a claim for damage done to insured property; or

g) In any other circumstances required under law or regulation.

iv. Where images are disclosed, a record will be made in the system logbook including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

v. Where images are provided to third parties, wherever practicable, steps will be taken to obscure images of non-relevant individuals.

7. Other CCTV Systems

i. The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its own School rules.

ii. Many students travel to School on coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The School may use these in establishing facts in cases of unacceptable student behaviour, in which case the parents/guardian will be informed as part of the School's management of a particular incident.

8. Complaints and Queries

i. Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the System Manager.

CCTV FOOTAGE ACCESS REQUEST

The following information is required before the School can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the School typically deletes CCTV recordings after 2 - 4 weeks.

Name and Address: (Proof of ID may be required)	
Description of footage (Including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (Give a range if necessary)	

Signature* ________________________________

Print Name ________________________________

Date ________________________________

***NB if requesting CCTV footage of a child under 13, a person with parental responsibility should sign this form. For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.**