MARLBOROUGH COLLEGE

INFORMATION, COMMUNICATION AND TECHNOLOGY (ICT) POLICY

Contents

INFORMATION, COMMUNICATION AND TECHNOLOGY (ICT) POLICY

Introduction

This information communication and technology (ICT) policy sets out the responsibilities, required behaviour and acceptable use for all users of the College's information systems, networks and computers including laptops and mobile devices.

1. **General Statement of the College's Duties and Scope**

Marlborough College (the College), incorporated by Royal Charter, is registered with the Information Commissioner's Office as a Data Controller. "The College" includes Marlborough College Enterprises Limited and additionally covers other subsidiaries and affiliated bodies.

All staff and pupils who have been granted access to use the ICT facilities together with anyone who may be granted permission to use the College's information, communication technology facilities and infrastructure (ICT) are subject to this policy regardless of the location of that person.

2. Definitions

- "Information communication and technology (ICT) covers all digital and analogue communications, telephone, data networks, internet connections, network and security infrastructure, data storage, data processing, servers, desktop computers, laptop computers, mobile devices such as iPhones and iPads, as well as all audio-visual equipment.
- "Users" is any person using the College's ICT infrastructure and equipment and includes all the people defined in more specific definitions, as well as any contractors, visitors, customers, volunteers and any temporary users of ICT.
- 'Pupils' is all persons studying at the college.
- 'All Staff' is all staff or employees of the College, including those on temporary or part time contracts and volunteers.

3. Accessibility of this document.

This policy is written using clear and plain language and is considered as age appropriate (Age 13 and above) for the accessibility of all ICT users at the College.

4. Your use of these networks, systems and devices indicates acceptance of this policy.

If you need help understanding this document or complying with any conditions, please visit the IT Help Desk or raise a support ticket.

Attention is also drawn to the existence of ICT Codes of Conduct, the Staff Code of Conduct and 'Rules of Custom – Mobile Devices' that also cover usage of ICT. The links for these documents are provided in this document.

5. Legal compliance and safeguarding

The College balances freedom of information, curriculum requirements with other statutory requirements, and filters or blocks access to some internet content, monitors and records usage and may process log files or other data to identify patterns of inappropriate behaviour.

It is illegal and therefore prohibited to use the ICT infrastructure, or any ICT equipment on College property, directly or remotely, for illicit purposes, including any involvement in terrorism-related activity or accessing extremist content outside of any explicit curricular purpose or for purposes of radicalisation.

All staff must be aware that filtering alone may not prevent access to all inappropriate or illegal content, and that other controls such as time-based access, supervision, education and pastoral care outlined in the Safeguarding Policy work together to prevent inappropriate behaviour, access to terrorist or extremist content and to prevent radicalisation in a manner compliant with the Government's Prevent Strategy.

6. User identification and authentication

Each user will be assigned an associated account password which must not be divulged to anyone, including ICT support services staff, for any reason. The College password should not be used as a password for any other service. All users are expected to remember their passwords and to change them if there is any suspicion that they may have been compromised.

Password strength is enforced, and passwords should be changed every three months, especially where Internet or public facing access to services is possible.

All staff will also be assigned a unique email address for his or her individual use. Users must not use the College email address assigned to anyone else without their explicit permission.

Email addresses are College owned assets and any use of these email addresses is subject to College policies.

7. Personal use of facilities and Bring Your Own Device (BYOD)

College information and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the College. Occasional personal use is permitted but only so long as:

- it does not interfere with the member of staff's work;
- it does not contravene any College policies;
- it is not excessive in its use of resources.

Reasonable personal use of College ICT infrastructure is permitted, for example the storage of personal photographs, videos, music collections and personal emails as well as appropriate gaming on either the College ICT infrastructure or utilising Cloud storage, provided they do not consume excessive resources, incur specific additional costs or impact other users.

All use of College ICT infrastructure, including any personal use, is subject to College policies. In particular all users are reminded they are responsible for ensuring intellectual property compliance and data protection compliance of all personal content, as well as maintaining personal backup strategies for personal data.

The College is not responsible for any loss or incidental loss arising from the personal use of its facilities, for example losses related to online banking conducted on a College PC or online banking application installed and used on a College mobile device or infrastructure.

All staff should use a College provided email account to conduct College business and should maintain a separate personal email account for personal email correspondence.

All users may bring their own device(s) and use them at the College. Devices may be connected to the College's network using individual Wi-Fi keys issued, or by using physical network points provided for that purpose.

The College may mandate the installation of mobile device management and other security software as part of the connection process. All devices used are subject to College electrical safety tests as required.

When connected to the College network or services, or when storing College data or programs on a personal device, all the ICT and Data Protection Policies apply to the use of that device.

The College has no liability for personal equipment. Users bring and use their own equipment entirely at their own risk.

When users leave the College, all College data and licensed software must be deleted from personal devices. Some software licensing arrangements may allow pupils and staff to take over accounts personally to maintain software subscription licences.

The ICT support group adopts a 'best effort' approach to supporting all BYOD devices.

Some personal devices are not permitted, personal network hubs or Ethernet switches must not be connected the network, and Personal Wi-Fi Access points are not permitted including using personal hotspots and 3G/4G mobile devices that transmit on Wi-Fi frequencies as access points, as these may interfere with the College Wi-Fi. The College may take steps to prevent these devices from functioning on College property.

8. Connecting devices to College networks

In order to reduce risks of malware infection and propagation, risks of network disruption and to ensure compliance with other policies it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the College's wireless networks using supplied individual credentials.

Every effort must be made to further reduce risks of data loss. All staff should not connect any personally owned peripheral device which is capable of storing data (for example a personally owned USB stick) to any College owned equipment, irrespective of where the equipment is located. Where such equipment is used, adequate data protection, antivirus controls, and encryption of personal or confidential data are mandatory and are the responsibility of the user to maintain.

Any device connected to a College network must be managed responsibly and effectively.

Under no circumstances should any unapproved network equipment be connected to the College infrastructure, this includes, hubs, switches, routers, Wi-Fi access points.

9. Mobile devices issued by the College

College owned mobile devices include phones, tablets, and laptop computers, and are issued with mobile device management and security software installed which must not be removed, these devices are subject to all the provisions in this policy.

Asset tracking of these devices, covering issue, return, and changes is controlled by the Electronic Asset Register, which is linked to the mobile management software.

These devices are valuable, and often contain valuable and confidential data. All staff must take good care of the mobile devices issued and take all reasonable precautions to ensure that they are not damaged, lost or stolen, and that appropriate security controls are in place at all times.

All staff must be mindful of additional usage costs with mobile network connected devices.

Mobile devices remain the property of the College, and all repairs must be facilitated via ICT support. Any incident involving damage, loss or theft of a mobile device must be reported immediately by creating a support ticket in the ICT system.

Negligent or repeated damage or loss of devices may be treated as misuse or abuse.

Attention is drawn to the presence of a Rules of Custom and ICT Codes of Conduct, and Staff Codes of Conduct:

Student ICT code of Conduct:-
Search on Firefly for 'ICT Code of Conduct', or use this link to view the latest code of conduct.
https://firefly.marlboroughcollege.org/student-it-services/using-it-at-marlborough/ict-code-of-conduct

Rules of Custom – Mobile Devices:-
Search on Firefly for 'Rules of Custom' or use this link to view the latest Rules of Custom for Mobile Devices.
https://firefly.marlboroughcollege.org/safeguarding--for-all-staff/rules-of-custom--mobile-devices

Staff Code of Conduct:-
Search on Firefly for 'Code of Conduct' or use this link to view the latest Staff Code of Conduct
https://firefly.marlboroughcollege.org/safeguarding--for-all-staff/safeguarding-and-child-protection-including-code-of-conduct-for-all-staff-and-volunteers

10. Incident management

Anyone uncovering a security vulnerability, experiencing a mobile device loss, theft or damage, data breach or data loss, or loss or compromise of credentials, has a responsibility to act immediately. Open an ICT support ticket or engage with the ICT support group as soon as possible.

Safeguarding incidents relating to ICT are reported and managed under the Safeguarding Policy. Issues relating to ICT must be co-ordinated with ICT support as soon as possible. The welfare of pupils as laid down by the College's Safeguarding Policy will always take priority.

11. Software

All software loaded on the networks or on computer systems belonging to the College must be properly licensed by the manufacturer and its use must conform to the terms of such licences. The following requirements must be followed:

- Users must not install software onto College computers for which the necessary licences have not been acquired.
- Care must be taken when making any copy of such software, or when enabling its use by more than one person, that the terms of any licences have not been breached.
- Software and other material downloaded and installed from the Internet must be licensed appropriately. The use of shareware software is always subject to a licence agreement, and acceptance of the terms of such a licence is implied when software is downloaded.
- The College does not condone or permit the unlicensed copying or use of software or other copyrighted material on computers belonging to staff or pupils, and the liability for the infringement of copyright in such cases is likely to rest with the individual concerned.
- In some cases, the College's licensing of software (Office 365 for example) allows restricted use on multiple devices including privately owned devices, and users must ensure they remain compliant with these licencing terms.

The College has the right to audit, by electronic and other means, the use of copyright software on any computer system belonging to the College. Any breach of these guidelines may result in disciplinary action.

12. Elevated Privileges

Some users will have elevated privileges allowing wider access to administer College services, or local systems, to enable self service of application installation, updates, or management of services.

When making use of these elevated privileges, users have a responsibility to exercise appropriate judgement in order to prevent damage or loss of data and credentials.

Users must not remove device management or security software from College equipment.

13. Use of services provided by third parties

Users must only use services provided or endorsed by the College for conducting College business. The College recognises however that there are occasions when it is unable to meet the legitimate requirements of its staff and pupils and that in these circumstances it may be permissible to use services provided by other third parties, where this is the case, adequate security must be in place and users must ensure there is no violation of data protection controls or infringement of legislation.

14. Unattended equipment

Computers and other equipment used to access College facilities must not be left unattended and unlocked if logged in. Staff must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended.

Particular care should be taken to ensure the physical security of all equipment and data when in transit.

15. Unacceptable use

In addition to improper control over unattended equipment, and for the sake of clarity, the following are also considered to be unacceptable uses of College facilities:

- Any illegal activity or aiding and abetting illegal activity or any activity which breaches any College policy. This includes any involvement in terrorism-related or radicalisation activity in line with the Government's Prevent Strategy.
- Any attempt to undermine the security of the College's facilities.
- Use of illegal hacking tools, stress testers, scanners, or other denial of service tools or exploits.
- Any attempt to remove or undermine the device management.
- Providing access to facilities or information to those who are not entitled to access.
- Any irresponsible or reckless handling or unauthorised use of College data.
- Any use which brings the College into disrepute.
- Any use of College facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited or unauthorised bulk email (spam) which is unrelated to the legitimate business of the College.
- Creating, storing or transmitting any material which infringes copyright.
- Creating, storing or transmitting defamatory or obscene material.
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of the College's facilities.
- Failing to report any breach or suspected breach of information security to ICT support.
- Failing to comply with a request from an authorised person for you to change your password.
- Failing to comply with data protection requirements.
- The use of VPN's and anonymizing / privacy applications.

16. Penalties for misuse

Minor breaches of policy will be dealt with by ICT Support. Heads of Department may be informed of the fact that a breach of policy has taken place. This includes negligent or excessive damage or loss of College assets.

More serious breaches of policy or repeated minor breaches will be dealt with under the College's disciplinary procedures.

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in the jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

17. Data protection and privacy

This section covers some key points of data protection and privacy as it relates to ICT, the Data Protection Policy covers all aspects of data protection including data protection outside the scope of ICT. All staff processing personal data must additionally comply with the current Data Protection Policy.

The College processes and stores personal data in compliance with current data protection legislation, all staff who have access to confidential, personal or personally identifiable data have a responsibility

to protect that data and protect access to that data, for example, not posting data in a publicly accessible place, using unsupported file sharing tools, using supported file sharing services inappropriately or storing data unencrypted on USB stick or external hard disk.

Please note that data protection also applies to all data whether or not it is stored, processed or accessed digitally.

Users, in particular all staff, also have a responsibility to protect data against irrecoverable loss by making adequate backups when such data is not stored in a secure College service. For the avoidance of doubt all important or sensitive data should be stored on College supported systems.

Under some circumstances it is permissible for the College to access the ICT accounts or monitor activity, communications and other data of an ICT user.

The College respects the privacy and academic freedom of its staff and pupils and recognises that investigating the use of ICT may be perceived as an invasion of privacy. However, the College may carry out lawful monitoring of ICT systems where there is sufficient justification to do so and when the monitoring has been authorised at an appropriately senior level.

Staff and pupils should be aware that the College may access records of use of email, telephone and other electronic communications whether stored or in transit. This is in order to comply with the law and applicable regulations, to ensure appropriate use of the College's ICT systems and to ensure compliance with other College policies. All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Retention and Investigatory Powers Act 2014, the Human Rights Act 1998 & Amendments, the Data Protection Act 1998 & Commencement Orders, (EU) General Data Protection Regulation 2016/679 (GDPR) and the Counter-Terrorism and Security Act 2015.

Decisions to access the IT accounts, communications and other data of staff and pupils will be taken by the Master or Director of Human Resources together with either the DPC or DPO in order to ensure that such requests are free from bias and are not malicious and compliant with current data protection legislation. Investigations of this kind are often sensitive and time-consuming.

Users may grant permission for ICT support to access data or desktops for the purposes of supporting a user with an issue, or fault rectification.

Log files and other activities may be processed or monitored for the purposes of impact on academic outcomes, pastoral guidance, safeguarding or identifying malicious or other incidents, or fault rectification or other security concern or incident. In particular, web site log files, firewall log files, Wi-Fi access log files, file server authentication and access logs are processed for all of these purposes to facilitate safeguarding requirements and assisting with lawful requests for data.

Data protection legislation requires that all staff and pupils access networks and systems using their own credentials.

- **The use of Electronic Mail**

  All staff should be aware that all inbound and outbound email are archived and may be reviewed internally if approved and may be required to be disclosed externally under some circumstances, for example compliance with a warrant, legal disclosure or data protection rights (Subject Access Request).

All staff should be aware that when sending an email message there is always a danger of the content being interpreted as official College policy or opinion. All e-mails will therefore be followed by the following disclaimer:

"Opinions, conclusions and other information contained in this e-mail that do not relate to the official business of Marlborough College shall not be understood as endorsed or given by the College. Any attachments are confidential and may be the subject of legal privilege. Any use, copying or disclosure other than by the intended recipient is unauthorised. If you have received this message in error, please notify the sender immediately and delete this message and any copies from your computer and network.

Marlborough College is neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt."

- **The College's Powers to Access Communications**

Authorised College staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or provided by the College and may examine the content of these files and any relevant traffic data or conduct covert monitoring when necessary.

The College may access files and communications for the following reasons:

- to ensure the operational effectiveness of its services, for example the College may take measures to protect its systems from viruses and other threats;
- to establish the existence of facts relevant to the business of the institution (for example, where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person);
- to investigate or detect unauthorised use of its systems;
- to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the College's business;
- to monitor whether or not communications are relevant to the business of the College (for example, checking email accounts when staff are absent on holiday or on sick leave to access relevant communications);
- to comply with information requests made under the Data Protection Act or Freedom of Information Act (individuals would in normal circumstances be notified);
- to support any safeguarding requirements, incidents or investigations;
- to comply with any additional lawful requests for data or information.

- **The Powers of Law Enforcement Authorities to Access Communications**

A number of other non-College bodies and persons may be allowed access to user communications under certain circumstances. Where the College is compelled to provide access to communications by virtue of a Court Order or other competent authority, the College will disclose information when required as allowed under the Data Protection Act 1998 or (EU) General Data Protection Regulation 2016/679 (GDPR).

For example, under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding issues of national security, the prevention and detection of serious crime or the safeguarding of the economic wellbeing of the UK.

- **Other Third Parties**

The College makes use of third parties in delivering some of its ICT services. These third parties may intercept communications for the purpose of ensuring the security and effective operation of their service. For example, a third party which provide e-mail services to the College may scan incoming and outgoing email for viruses and spam, or a Cloud service provider may comply with a lawful order for access to information stored in the 'Cloud', which may be subject to different jurisdiction.

- **Procedure**

Requests for investigation under this policy may be made by any member of staff although typically the request will come from a Head of Department. Occasionally requests are made from outside of the College, for example by the police. The request should be made to the Master or Director of Human Resources and should include the following information:

- the name and department or House of the staff member or pupil whose computer or computing activity you wish to be investigated;
- the reasons for the request;
- where computer misuse is alleged, the evidence on which this is based;
- the nature of the information sought;
- any other relevant information, for example that the request relates to an ongoing disciplinary or grievance procedure.

All subject access requests (SAR) made under data protection legislation must be processed and co-ordinate by the Data Protection Controller (DPC) or data protection officer (DPO). Please refer to the Data Protection Policy for full details.

In order to monitor the number and type of requests made, the College's Human Resources Department will keep a record of the requests that have been made and those which were agreed.

Author: Director of Corporate Resources
Date: Summer Term 2018
Review: Summer Term 2019