MidKent College
ICT Policy

Document Details			
Policy Number	**MKC-ICT-001 - 6**	**No. of Appendices**	
Document Title	**ICT Policy**		
Document Description	*Staff and students accessing ICT devices and internet.*		
Effective Date	**September 2022**	**Review Date**	**December 2026**
Version Number	**V1.3**	**Review Cycle**	**2 years**
Document Status	**Approved**	**New Policy**	**N**
Change Criteria	**Minor**		

***Major change is defined as:**
Anything that represents a significant change of working practice, legal requirement, procedure or process within the organisation, or a change that impacts an employee's terms and conditions of employment.

***Minor change is defined as:**
Any change of dates, job titles or terminology that do not represent a significant change to working practice. Examples changes of terminology to reflect current legislation/ DfE/Ofsted such as the change of terminology in the safeguarding policy from peer-on-peer abuse to child-on-child abuse.

Document Authorisation				
	Authorisation Required	**Initial and Role**	**Digital Signature**	**Date**
Author	Yes	Paul Hogben Group Director of ICT		
Owner	Yes	Paul Hogben Group Director of ICT		
SLT Review	Yes/No			
Exec Approver	Yes	Chris Hare, Deputy CEO and Executive		
GB Sub Committee	Yes/No			
Full GB Committee	Yes/No			

Policy Cross References - This policy should be read in conjunction with any other associated policies, with particular reference to	
Policy Name	**Policy Number**

Document Revision History		
Version Number	**Date**	**Summary of Revision**

Contents

1. Introduction

1.1. This policy defines the acceptable use of all ICT resources within the College and is supported by the Data Protection Policy to ensure the security of College data and our users' personal information.

2. Scope and Aim of Policy

2.1 This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by MidKent College or any of its subsidiary companies (known as the "MidKent College Group", the employee, or a third party. All MidKent College or MKC Training Services Ltd, any other subsidiary companies, employees, students, contractors, consultants, temporary, and other workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, local laws and regulations.

An overarching rider document can be appended to this College Policy to identify criteria that is not relevant to MidKent College Group subsidiaries or any other subsidiary companies. Each rider is to be signed by the Director of ICT and a relevant position responsible for technology within the subsidiary, to confirm validation of the caveats identified.

3. Procedures

3.1 Acceptable Usage Statement

ICT facilities are provided for the purpose of fulfilling the educational objectives of the College and to assist studies or work. It is impossible to define every specific allowed use, but examples of acceptable use include research for assignments and assessments, using online learning materials, participating in appropriate discussion groups, or completing work on behalf of the College.

All statements below are identified as actions deemed as unacceptable use. Users must not:

3.1.1 Create, access or transmit any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

3.1.2 Create, access or transmit any material of a sexist or racist nature, or any other material in contravention of the Equality Act 2010, or material of a libellous or of a terrorist nature.

3.1.3 Create, access or transmit any material in violation of any United Kingdom law or College policy. This includes, but is not limited to, copyright material, threatening or obscene material.

3.1.4 Use College systems for private business activities or product advertisement.
3.1.5 Access material that involves extremist organisations and/or promotes beliefs contrary to British values. As required under the UK government Prevent strategy.
3.1.6 Bring the College into disrepute through creating or transmitting material or through online, ‘social networking’ activities.
3.1.7 Transmit unsolicited, commercial or advertising material to other users.
3.1.8 Use or produce materials to attempt to gain unauthorised access, or make unauthorised changes to the College ICT facilities, or those of other organisations. This includes network scanning or probing activities.
3.1.9 Create, access or transmit material which is designed to, or likely to cause annoyance, inconvenience and/or needless anxiety.
3.1.10 Create, access or transmit material which is designed to be defamatory.
3.1.11 Transmit material or use software which infringes the copyright or intellectual property rights of another person or third party.
3.1.12 Download, copy, store or supply copyright materials including software and retrieved data without the permission of the Copyright holder or under the terms of the licence held by the College.
3.1.14 Engage in deliberate activities with any of the following characteristics:
- Corrupting or destroying other users' data.
- Violating the privacy of other users.
- Disrupting the work of other users.
- Preventing others from accessing a workstation when they are no longer using it, including locking workstations.

3.1.19 Continue to use an item of networked software or hardware after the College has requested that use cease because it is causing disruption to the correct functioning of the network.
3.1.20 Engage in other misuses of the network or networked resources, such as the introduction of 'viruses'.
3.1.21 Play online games other than those created for learning purposes and authorised by the ICT Department.
3.1.22 Use chat-sites unless authorised by the College.
3.1.23 Allow their account to be used by others or disclose their passwords to others.
3.1.24 Use accounts or passwords belonging to others.
3.1.25 Engage in software theft or abuse of software licenses.
3.1.26 Forge e-mail signatures or use College logos for unauthorised purposes.
3.1.27 Attempt to open, move, disconnect or in any other way tamper with or attempt to destroy or damage ICT equipment. All faults with equipment should be notified to the ICT Department through the ICT Helpdesk. Students are advised to contact their tutors regarding ICT equipment.
3.1.28 Access College resources from an untrusted or unsecured source, as defined by the ICT department.
3.1.29 Other examples of misuse include, but are not limited to, uploading images or videos which show antisocial behaviour or illegal activities; making derogatory statements about the College, College staff or College students; or revealing confidential information about the College, College staff or College students. You are prohibited from knowingly accessing, viewing or downloading such materials.

3.1.30 Purchase software without permissions being obtained by ICT directly. Purchasing software personally will not be reimbursed by the College, even if the sole purpose of the purchase is for College use.

3.2 Information Security & Data Protection

Strategies and technology are implemented to ensure the security of all entities of the organisation by protecting our network and our users. The following policy statements outline the commitments from the College to ensure a safe environment.

3.2.1 Approved Storage Locations

Below are all the approved storage locations for data within the College:

OneDrive: Microsoft OneDrive is provided as part of the College Microsoft subscription. All authorised users are provided with 1Tb (Terabyte) cloud storage which is accessible from the web interface, OneDrive sync client and OneDrive Connect (providing N:\ for all users). Links that are shared anonymously from OneDrive will expire after 180 days. College OneDrive accounts are not for personal use and should not be used to save personal files that are not related to the business.

SharePoint 2013: Microsoft SharePoint 2013 is our current storage location for all corporate documentation. SharePoint is hosted within our organisation (On-Premises).

SharePoint Online (Cloud): Microsoft SharePoint Online is provided as part of our Microsoft subscription. The College will be migrating SharePoint 2013 to this platform. Software like Microsoft Teams and Office 365 applications use this as a storage location. Links that are shared anonymously from SharePoint Online will expire after 180 days.

File Servers: File servers can be accessed only by those given explicit rights by the ICT department. This data is hosted within our organisation (On-Premises).

Virtual Learning Environment (VLE): The College Virtual Learning Environment hosts course related content for our students. This is hosted within our organisation.

3.2.2 Device Encryption

College devices will be encrypted where possible using the current encryption technologies. Device encryption for College devices will conform to the following standards:

Student Desktops: Disk drives will be encrypted to XTS AES256 standard and

network unlock is configured. Network access will be required for the machine to be unlocked and used.

Student Mobile Devices: Disk drives will be encrypted to XTS AES256 standard.

Staff Desktops: Disk drives will be encrypted to XTS AES256 standard and network unlock will be configured. Network access will be required for the machine to be unlocked and used.

Staff Mobile Devices: Disk drives will be encrypted to XTS AES256 standard. PIN numbers may be required on devices that do not confirm to the technologies to enable encryption.

3.2.3 Role Based Permissions

Role-based permissions are a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job title, department, and responsibility within the College. These permissions are defined on criteria from the HR system.

3.2.4 Windows Updates

Windows Updates are centrally managed by the ICT department using System Center Configuration Manager (SCCM) to ensure effective patching of network systems. Updates are released monthly and conform to the guidelines in the 'Windows Update Procedure' produced by ICT.

3.2.5 Virus & Malware Protection

All College systems require Antivirus software to ensure protection against emerging virus and malware attacks. This is centrally managed by the ICT department using SCCM Endpoint Protection. Malware definitions are automatically updated and deployed daily to all College systems.

3.2.6 Removable Storage Devices

The use of USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications as storage devices such as mobile phones, PDAs, etc. has also increased. They are highly susceptible to loss, theft or infection. To ensure the protection of organisational and personal information the College will enforce the following:

- All removable storage functions will be disabled on all College devices by Group Policy.
- An exception list will be managed by the Information Security Group to

ensure those who require this function are not restricted but are recorded and a risk rating assigned.

- Corporate owned encrypted pen drives may be provided to staff or students where applicable after a data protection assessment of their needs.

3.2.7 Accessing College Resources from an Untrusted Source

If a users' account is identified as having tried to access College resources from a source that is deemed untrusted by the ICT department, the account will be instantly disabled, and the user will be contacted. This is to ensure the security of the network. An untrusted source could be, but not limited to the following criteria:

- A personal computer that does not have the following system requirements:
  - Up-to-date operating system
  - Anti-Virus installed
- A logon from an untrusted IP address or location
- Multiple failed logons from the same location

To ensure that devices are not untrusted Cyber Essentials Plus requires that all staff devices that are connected to orgnisational data are required to register their device on the College Mobile Device Management platform (intune) and must be running a minimum manufacturer supported operating system. All devices that are not compliant will be blocked for access College organisational data.

3.2.8 Microsoft Local Administrator Password Solution (LAPS)

Microsoft Local Administrator Password Solution is required to randomize the local administrator accounts on all client machines to reduce the risk of a client side infiltration attack. The software is centrally managed by Group Policy and applies to all staff, student and server machines (excluding Hyper-V hosts and Domain Controllers). Access to these passwords is restricted to ICT staff only.

3.2.9 Multi-Factor Authentication (MFA)

Multi-Factor authentication uses a secondary device which is personal to the user to help validate their identity. High risks accounts will be targeted, where applicable, to utilise MFA technology. All members of the College Executive Team, Senior Leadership Team, ICT and Data Protection are required to use MFA to access College resources.

3.2.10 Internal & External Email Attachments

To minimise the data that is held within our Exchange environment, to support collaboration and ensure that we information security requirements are upheld, internal and external email attachments are disabled. This applies to all staff

and exceptions are approved via an internal approval process managed by the information governance team.

3.2.11 Website Security

This section defines the security requirements that need to be in place for any website of College system that hosts or holds College data or information.

External Facing Websites (Internally hosted and publicly accessible or externally hosted)

- All sites to have a current public SSL Certificate.
- All Sites to conform to PECR (aligns with cookies, privacy notices).
- All sites to have been penetration tested where possible and aligned with CE+ requirements.
- All sites should conform with College branding standards.
- All sites, where data is collected, need to be approved by the Data Protection Officer and align with the College Data Protection Policy.
- The Director of ICT/ Director Of Marketing/ Data Protection officer can enforce the removal of web sites that do not conform to the standards above.

Internal Facing Websites (Sites created internally for internal use)

- All sites to have a current Internally signed SSL Certificate.
- All sites to have been penetration tested where possible and aligned with CE+ requirements.
- All sites where data is collected need to be approved by the Data Protection Officer and align with the College Data Protection Policy.
- If applicable, Single Sign On (SSO) is enabled.
- The Director of ICT & Data Protection officer can enforce the removal of web sites that do not conform to the standards above.

3.3 Active Directory Accounts

3.3.1 Staff Accounts

3.3.1.1 **Account Creation**

All new staff at MidKent College provide their personal details to HR. HR provide the following information to ICT so that a network account can be created:-

- First Name
- Surname
- Department
- Main Campus
- Line Manager
- If a Teams DDI (phone) is required

- If a PGCE placement – details of the mentor and an expected end date
- If a Temporary member of staff – details of the expected end date

ICT will use either the full name or known as name provided by HR for Active Directory account information. This is agreed with HR.

Once the above information has been collected the ICT department will perform the following tasks:

- The Active Directory account will be created using the initial of the first name along with the surname, to create a unique login username. If the login username is not unique the next character of the first name is also used, this repeats until the username is unique. This will allow access to the computer network.
- A Teams account will be created, giving access to the Teams system and a DDI created if requested through the ICT Helpdesk.
- An Equitrac printing system account will be created, used in conjunction with the staff ID card to release information sent to networked printers.
- A helpdesk system account will be created, allowing staff to raise, update and monitor progress of support calls.
- A password will also be created for the account. These account details will be provided to the manager for when the staff member starts at the College.

3.3.1.2 **Account Removal**

- When a staff member leaves the College their ICT account will be automatically disabled overnight. This is based on information within the HR system.
- Access to staff leavers data is managed by Data Protection. ICT will never provide access to an account without this authorisation.

3.3.1.3 **Departmental Changes**

HR will notify ICT when staff move between departments. They will provide the following information: -

- Full Name
- ERN
- New Department
- New Site
- New Line Manager
- Date of moving

If the move involves changing site, the current telephone extension may be changed to a new extension relevant to the new site.

Once an account has been created all information excluding the staff members name and ERN will be synchronised with the HR database making this the primary source of Staff Account information.

Employees who change roles whilst under contract with the College will retain their existing user account, however the permissions and access levels applied will be subject to change to reflect the requirements of the job role. Employees will continue to have access to e-mails in their mailbox that relate to their previous role in line with the College's Retention Schedule.

Employees who change roles but have a gap in employment will lose access to their College account between the end date of the previous contract and the start date of the new contract. On return, employees will be re-gain access to their account and will have access to e-mails in their mailbox that relate to their previous role in line with the College's Retention Schedule.

Employees who leave but subsequently return to the College as an employee will be provided access to their previous account; (providing the return date is within 7 years of the previous leaving date. On return, employees will be re-gain access to their account and will have access to e-mails in their mailbox that relate to their previous role in line with the College's Retention Schedule. The permissions and access levels applied will be amended to reflect the requirements of the new job role. In the circumstance that a previous employee leaves and returns as an employee over 7 years later, a new account will be created.

Employees who leave but subsequently return to the College as a contractor will be provided with a new account. Contractors who return/transition to the College as an employee for an identical role, will be given access to their previous account, including access to e-mails in their mailbox that relate to their previous role in line with the College's Retention Schedule. In the circumstance that the contractor returns/transitions to the College for a different role, a new account will be provided.

The Director of People, Director of ICT and Data Protection Officer reserve the right to overrule any of the above if mitigating circumstances apply. Mitigating circumstances include but are not limited to: legal proceedings, conflict of interest, significant changes to a job role that result in access to information that the postholder would not normally have access to.

3.3.1.4 **Stale Accounts**

ICT will run monthly checks on staff accounts. If there is no activity for 3 months the following is performed:

- Contact HR to confirm if the users are still active staff.
- If HR confirms the user is no longer present the account is then removed following the ICT account removal procedure (3.3.1.2).

If an account shows as past the agreed contract date the Active Directory account will be disabled.

3.3.1.5 **Restricting Accounts & Investigations**

ICT will only disable a Staff account or access to the internet for a staff member, or undertake an investigation, if the request comes directly from the HR Team or an Executive Director. ICT will deny all requests from any other party other than those listed above.

3.3.1.5 **Staff Absence**

There are occasions when staff are absent from the College for an extended period of time (e.g. Maternity Leave, long term sickness etc.). HR will advise ICT when any member of staff is expected to be away from the College for an extended period of time and will advise how ICT should proceed. The following information may be required to process this request:

- First Name
- Surname
- Department
- Line Manager
- Estimated date of return to work
- ICT will mark the Active Directory record for that user to ensure that it is not disabled or removed as part of the Stale Account process above.

HR are not required to specify the reason for absence.

3.3.2 Student Accounts

3.3.2.1 **Account Creation**

All new students to the College have their accounts automatically created on completion of enrolment within our Student MIS system. The following information is required to create the account:

- Enrolment Number
- First Name
- Last Name
- Level

3.3.2.2 **Account Removal**

The list of active enrolled students are identified by the student MIS system and then compared to the list of Active Directory accounts. If it finds that the student is no longer enrolled within the College the account is automatically disabled. Student accounts are removed after 18 months.

3.3.2.3 **Restricting Accounts & Investigations**

ICT will only disable a student account or internet access for students, or undertake an investigation, if the request comes from a Curriculum Director or from the College Safeguarding team. If a member of staff directly requests this from ICT, ICT will deny this request and will require a discussion between the staff member and the approvers above before any action is undertaken. This will allow for any curriculum processes to be undertaken before the action of disabling, restricting or investigating an account.

3.3.3 Contractors, Consultants & College Affiliates

There are instances where people external to the College require login accounts to access College resources. The following processes are followed in these instances.

3.3.3.1 **Account Creation**

HR provide a list of 'Long Term Contractors' to the ICT Helpdesk. The following fields are required:

- First Name
- Surname
- Department
- Main Campus
- Line Manager
- If a Teams DDI (phone) is required
- Expected end date

3.3.3.2 **Account Removal**

HR provide a list of 'Long Term Contractors' for removal from Active Directory. On submission of this request all ICT accounts are disabled, and all rights are removed.

3.3.3.3 **Restricting Accounts & Investigations**

ICT will only disable a Long Term Contractor account or access to the internet, or undertake an investigation for a long term contractor if the request comes directly from the HR Team or an Executive Director. ICT will deny all requests from any other party other than those listed above to disable accounts.

3.3.4 Password Policy

3.3.4.1 This policy defines the specific requirements for all users based on the complexity, length, characters and expiration of their password. This also

defines the account lockout times based on incorrect password submissions. This is based on current government advice for all business and institutions. (https://www.cyberaware.gov.uk/passwords).
The following settings are applied in Active Directory:

Password Policy	
Enforce Password History	24
Maximum Password Age	365
Minimum Password Age	1
Password Minimum Character Length	14
Password Must Meet Complexity Requirements	No
Account Lockout Policy	
Account Lockout Duration	15 Minutes
Account Threshold	10 Attempts
Reset Account Lockout Counter After	15 Minutes

3.3.4.2 Below is a list of all the settings listed above and their definitions

Enforce Password History: This security setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.

Maximum Password Age: This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it.

Minimum Password Age: This security setting determines the period of time (in days) that a password must be used before the user can change it.

Password Minimum Character Length: This security setting determines the least number of characters that a password for a user account may contain.

Password Must Meet Complexity Requirements: This security setting determines whether passwords must meet complexity requirements. The standard Microsoft complexity rules state that the minimum requirements must be met: It must not contain user's account name or parts of the user's full name that exceed two consecutive characters. Be at least 6 characters long. Contain characters from three of the following four categories: English uppercase characters, English lowercase characters, Base 10 digits, Non-alphabetic characters. Complexity requirements are enforced when passwords are changed or created.

Account Lockout Duration: This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked.

Account Lockout Threshold: This security setting determines the number of failed logon attempts that causes a users' account to be locked out. A locked-

out account cannot be used until it is reset by an administrator or it reaches the lockout duration for the account has expired.

Reset Account Lockout Counter After: This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon counter is reset.

3.3.4.3 **Password Advice**

Never use the following personal details for your password:

- Current partner's name
- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team

3.3.4.5 **Password Management**

Passwords can **only** be stored in a centralised password manager, managed by ICT. Methods list below, but not limited to, are defined as a security risk to the organisation:

- Hand written notes or stickers
- Excel spreadsheets / Word documents (including those password protected)
- Stored within emails
- Verbally shared

Heads Of Department will be responsible for managing their own password lists with the oversight of ICT to ensure password security.

3.3.5 Shared User Accounts

A shared user account is a logon account that is designed for multiple people to use simultaneously providing access to a resource or service. Use of shared accounts are to be restricted to ICT only due to the high security risk they incur. ICT reserve the right to disable existing shared accounts where applicable.

3.4 Printers

There are a number of printers available across the College which are available for Student and Staff use. The printers offer the following functionality:

- Printing
- Scanning
- Copying

3.4.1 Printer Access

All printers can be operated by the following methods:

- ID card.
- Username and password

ICT help desk will support printer issues when provided with the location of the printer and the name and/or serial number of the device.

Printing documentation at home or from non-authorised devices is not permitted, with machine policies in place to restrict this feature.

3.4.2 Printing Costs

Print balance are associated to the individual's department and shared with all members of the department. This balance can be seen on the printers. The print charges are as follows:

- A4 B&W – 2p
- A4 Colour – 15p
- A3 B&W – 4p
- A3 Colour – 30p

B&W and Duplex is the default for all printers, but this can be overridden by each user.
Students have their balances set at the start of each academic year (regardless of whether they are a new student or existing) as follows:

- Level 1 students - £40
- Level 2 students - £50
- Level 3 (and above) students - £60+

Students can top up their balances if they run out of credit by paying for additional credit at the Finance desk in the reception areas or in any of the Learning Resource Centres (LRCs)

3.4.3 Scanning

All printers have the ability to scan a document using the "scan to me" function. They can be operated by an ID card as supplied by the College along with the staff/students PC log in details.
The scanners offer the functionality:

- Scan to Network Share.
- Scan to SharePoint.
- Scan to OneDrive.

3.4.4 Copying

All printers have the ability to copy a document and can be operated by an ID card as supplied by the College along with the staff or student logon details.
The copier will offer the functionality to amend the size, duplex, colour output of the document being copied.

3.5 Allocation of Desktop, Laptops and Tablets to Staff.

3.5.1 Upon request, ICT will allocate the appropriate Desktop, Laptop and/or Tablet depending on the individual's job role requirements.

3.5.2 Teaching staff who deliver a minimum of 10 hours of teaching per week, or those who support teaching and learning in the classroom environment for a minimum of 10 hours per week, will be allocated a laptop that conforms to the minimum specification.

3.5.3 ICT loan laptops can be made available for short term loan or ad-hoc provision for staff that do not fulfil the hourly entitlement.

3.5.4 Every Windows based computer, inclusive of laptops, issued by ICT will conform to ICT's minimum standard specification as follows:-

- Intel i5
- Intel i3 (where applicable)
- 8Gb RAM or greater
- 120Gb SSD or greater
- Gigabit Ethernet adaptor (where applicable)
- 802.11ac dual band wireless network card (where applicable)
- TPM or equivalent technology
- USB C compliant

3.5.5 Where staff are not entitled to a laptop under point 3.5.2 a desktop computer will be made available. Should a laptop be the preferred device, then a clear Teaching, Learning & Assessment benefit will need to be demonstrated and have approval from relevant head of department. ICT reserve the right to charge a proportional value between the costs of a new laptop and new desktop to the department.

3.5.6 Any computer equipment purchased by the College will fall under the remit and management of ICT regardless of department or budget used to purchase and as such, ICT reserve the right to re-allocate a device that is identified as being not fully utilised in conjunction with the user and department manager.

3.5.7 Should a budget holder request a device outside of the minimum specification then a clear Teaching, Learning & Assessment benefit will need to be demonstrated and have approval from relevant head of department. ICT reserve the right to charge a full value of the device to the department. Furthermore, the device must conform to the minimum specification and be from a preferred purchaser list.

3.5.8 Should a current or new member of staff require a device for Health and Safety reasons, the request should be approved by HR and their line manager. ICT will then facilitate the request.

3.5.9 All staff will be issued with a laptop bag, headset and presentation adapter when being issued with a laptop. Staff are expected to use the issued laptop bag when transporting their laptop between meetings/sites/rooms etc. Any damage caused as a result of misuse, lack of care or neglect may result in disciplinary action based on HR protocol.

3.5.10 All staff are expected to look after the equipment issued to them. Any damage caused as a result of misuse, lack of care or neglect may result in disciplinary action based on HR protocol.

3.5.11 Staff on long term absence may be asked to return their device for the duration of their absence, in conjunction with HR protocol. This device will be allocated to their replacement or go back to College wide deployment.

3.5.12 College equipment is to be used only to complete work for MidKent College. It is not acceptable for College equipment to be used for personal usage or for personal gain.

3.6 Student IT Suites, Laptops & Tablets, Trolley & Lockers

3.6.1 Protection of Hardware

It is the responsibility of every department to ensure the correct and safe use of computer hardware to ensure that teaching and learning is not detrimentally affected. The following rules should be followed:-

- When not in use, IT Suites are locked and no students are left unattended.
- When not in use/unsupervised, laptop trolleys are locked in a classroom/office.
- Laptops should be stored in the trolley to ensure ease and efficiency of use.
- Laptops, when not in use, they should be plugged in to the integral power supply in the trolley.
- All laptops should be switched off correctly at the end of each session and returned to the trolley.
- The trolley should remain plugged in to the mains supply whenever possible, and certainly when being stored/not used for any length of time.
- Sharing trolleys or laptops between multiple classes is not considered best practice.
- Students/staff should not carry laptops by the screens or have fingers on the screens.
- Care should be taken when moving trolleys around the College and this should be supervised by staff.
- At the start and end of each session of use, the laptops should be counted to ensure all devices are accounted for. Any issues should be reported to the ICT helpdesk immediately.
- ICT reserve the right that costs related to the upkeep of the trolley, such as replacement of missing laptops, laptop chargers, repair of damaged devices, to be charged to the department.

3.6.2 Fault reporting

Any issues with the computers/laptops/tablets/trolleys should be reported to ICT helpdesk immediately. Upon receipt of a fault, ICT will define whether the damage is to be classed as ‘wilful damage’ or ‘general wear and tear’. These issues include, but are not limited to the following:

- Missing laptops
- Damaged equipment including trolleys
- Equipment not allowing students to login
- Trolley not charging
- Broken Screens/keyboards
- Generally not working
- Missing power supplies
- Mains cable damaged or missing

Should the individual responsible for the trolley leave employment at the College then ICT will work with the HOD to identify a new responsible staff member.
ICT will audit the Trolleys on termly basis and report to the HOD's on the quality of the trolley.
Should a cause for concern need to be raised as a result of an inspection, the engineer will evidence the findings and raise a cause for concern escalation.
Following on from a trolley audit, or where ICT have been made aware of breaches to some or any of the above "rules" or where the devices are not being effectively managed or utilised, ICT reserves the right to remove from a department some or all of the issued trolleys and the associated laptops. Any device removal will be in conjunction with discussions with the Head of Department and/ or Director of Curriculum.

3.6.3 **Best Practice**

The following statements identify best practice and recommended usage:

- Identify a member of the department to take responsibility for certain trolleys.
- Departments use booking systems to manage trolley allocation. These can be setup upon request to the ICT Helpdesk.
- All trolleys and their associated laptops should be kept together within the same room. All laptops should be returned to the trolley that they were originally removed from. It is best practice to use the trolley(s) which have been allocated to the department.
- Any requests for support should be reported to the responsible person as well as ICT helpdesk.
- Charger wires should remain in the laptop tray and not be removed.
- All laptops are numbered/labelled and the laptops should be returned to the relevant shelf.
- Trolley laptops are for the benefit of the students. Staff should refrain from using them for teaching purposes. Loan laptops for this purpose are available from ICT.
- IT Suite assignment is managed by timetable booking with MIS.

3.6.4 **Direct Issued Devices**

For directly issued devices, the student is held responsible to ensure a high

standard is maintained. A contract will be issued clearly stating the terms of the device allocation.

Devices that are directly issued to students are liable for recall for the following reasons:

- Maintenance
- Security issues
- Misuse
- Change in scheme or allocation
- End of Study

3.7 IT Asset Management

This section of the policy governs the purchasing and disposal of hardware and software within the College. Purchasing of equipment must conform to the principles outlined in the ICT Strategy for Supporting Teaching, Learning & Assessment.

3.7.1 Suppliers

- Preferred/contracted suppliers are chosen through a formal tender process to supply personal computers, including desktop, notebook and server systems.
- Supplier maintenance and service availability as well as product warranties will be taken into account in the purchasing decision.

3.7.2 Software Procurement

- ICT is responsible for the full range of software licensing across the College.
- All new and upgrade software requests are to be raised on the ICT Helpdesk along with supporting reasoning for the purchase in order to ensure compatibility with existing systems, reduce multiple purchases and ensure best value.

3.7.3 Environments

- The Windows operating system environment will be the standard desktop environment for desktop and laptop systems.
- The College portal page will be the only supported desktop computing environment to provide full access to the College corporate systems.
- ICT will maintain specifications of recommended desktop and notebook hardware for systems that run a Windows desktop operating system.

- Servers on the College network will run on a Microsoft Windows server operating system. For a limited range of specialist tasks other server operating systems may be used following consultation with ICT
- Other operating systems will be supported where demonstrable that the Windows operating system is not suitable.

3.7.4 **Asset Control**

- ICT will be responsible for maintaining records of the computer systems.
- ICT will be responsible for maintaining records of RFID chips of computer systems issued to MidKent College.
- ICT will be responsible for warranty records or similar.
- ICT will be responsible for maintaining software records to meet obligations to software vendors under licensing contracts.
- All equipment owned by the College will be managed by ICT and issued based on an identified criteria for use irrespective of the department from whose cost code it was originally purchased.
- When a device is issued the device and relevant user details will be updated within the ICT Helpdesk system. This information can be used for location and identification of the registered user consequently the device must not be passed to another user without the express knowledge and approval of ICT.
- In general terms, all equipment issued must be returned to ICT when no longer needed for its intended issued purpose. Reasons for this could be, but not limited to, change of job role, user has left the College, etc.
- All College equipment will follow the naming structure defined in the Naming Convention Procedure

The Lawful Business Practice Regulations, which came into effect on October 24th 2000, allow organisations to monitor or record all communications transmitted over their systems without consent for the following purposes:

- Establishing the existence of facts.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures (i.e. ascertaining whether the business is abiding by its own policies).
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and staff training).
- Preventing or detecting a crime.

- Investigating or detecting unauthorised use of the business's telecommunications system.
- Ensuring the effective operation of the system.

The Regulations also authorise businesses to monitor (but not record) communications for the following purposes:

- Checking whether or not communications are relevant to the business
- Monitoring number of calls to confidential counselling helplines run free of charge.

3.7.5 Asset Relocation

Assets will be relocated within MidKent College during breaks in College terms. This is to reduce the amount of disturbance caused and the time required for ICT to successfully implement the change. This is inclusive of all staff office moves. The **ONLY** time assets will be relocated during term time will be if the relocation directly impacts an improvement in the teaching and learning experience.

3.8 ICT Purchasing Budgets

ICT will be responsible for the procurement of all computer equipment within the College, in line with the financial regulations, and all equipment must be purchased through ICT to ensure that it meets the minimum requirements and is secure and appropriate for the College network.

ICT will be responsible for the procurement of all software within the College, in line with the financial regulations, and all software must be purchased through ICT to ensure correct network licensing and system compatibility. All proposed software purchases will require approval for the Director of ICT and must be aligned with the presented business case for that department. The software MUST align with the Data Protection policy.

Any other item that requires a connection to the College infrastructure needs to be confirmed by ICT for network compatibility.

3.9 Waste Electrical and Electronic Equipment (WEEE)

Any equipment that is either damaged or redundant is sorted into the following categories:

- Items for sale
- Items for disposal

Items for sale are sold as part of 'Buy Back' Schemes allowing ICT to recuperate the cost towards the replacement device. A certificate or receipt is expected for the sale of an item. **Items for disposal** are stored in cages in the ICT store rooms. When full, a ticket is booked for facilities to collect and their contractor takes it away.

3.9.1 Hard Drive Management and Destruction

Redundant physical hard drives (HDD) will be disposed of aligned with our Data protection requirements. This destruction will meet the standards required in the Data Protection Act 2018.

Redundant Solid State Hard Drives (SSD) will be stored in a locked area for reuse within College devices. All data will be removed from the SSD at the point of storage. Any SSDs that reach their end of life will be removed in line with the HDD standard.

3.10 Web Content Filtering

The filtering of both the internet and indeed any College programme content provides an important means of preventing users from accessing material that is illegal or inappropriate for education. This helps to manage the associated risks and to provide preventative measures which are relevant to the College. This ensures that the College is meeting its duties under the PREVENT legislation and safeguarding requirements for all students.

3.10.1 **Responsibilities**

- The responsibility for the implementation of the College's filtering policy will be held by the Director of ICT. The filtering system will store 3 months of historical usage data.
- All users have a responsibility to report immediately to the ICT Helpdesk any infringements of the College's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. If this involves a sensitive/confidential matter then this should be reported directly to the ICT Technical Support Manager.

3.10.2 **Policy Statements**

Below are policy statements compiled by the ICT department to ensure effective web filtering protection:-

- Internet access is filtered for all users. The content filtering system provides customised levels of filtering in order to facilitate flexible teaching and learning practices.
- Illegal content is filtered by the Internet or filtering providers by actively employing the Palo Alto K12 Education content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the College to breaches of the filtering policy.
- There is a clear route for reporting and managing changes to the filtering system.
- The College maintains and supports the managed filtering service.

- Any filtering issues should be reported immediately to the ICT Helpdesk.
- Requests from staff for sites to be unblocked will be considered by the technical staff. If the request is agreed, this action will be recorded.
- If the ICT Helpdesk is unsure whether content should be unblocked this is passed to the Safeguarding Team to confirm the status of the web page.
- Daily reports are run and sent to the Safeguarding Manager for review. These list internet searches using key suspicious phrases and detail (on College equipment) both the machine used and the user id.
- Any user searching on the internet will be forced to "SafeSearch" where inappropriate content is removed.
- The College also monitors computer activity by both staff and students not only on the internet but across all College applications. This is done using the computer monitoring system. The system monitors key presses and keywords against a phrase list. This list includes all areas of Safeguarding and radicalisation to meet Prevent responsibilities.
- The Safeguarding manager also accesses the dashboard of the computer monitoring system where breaches are categorised and assigned to risk levels.

3.10.3 **Security Features**

The following features are part of the web filtering service provided by the Palo Alto firewall system:

- Wildfire – Deep packet inspection that looks to identify and execute malicious code in packets as they pass into the College network.
- Threat protection – Live protection that identifies threats in College network traffic.
- SSL Decryption – Decryption of secure web pages allows the College to view content previously encrypted with HTTPS protocols. This allows URLs to be capture and information transmitted to be checked and recorded. We do not SSL decrypt the following categories:
    - Banking
    - Health
    - Personal Communication

3.11 Mobile Phone and Mobile Device Policy

3.11.1 **Provision of Mobile Devices**

The College provides a mobile phone for specific post holders. The criteria and justification for issue of a mobile phone is as follows:

- A staff member must be actively travelling between College sites or to designated areas where communication equipment i.e. internal phone or computer is not available;
- The member of staff's position requires immediate communication;

- Staff that need to be contacted to ensure the continued operation of College facilities, College equipment and/or College infrastructure would be considered eligible.

3.11.2 **Service Provision**

- All College mobile phones are on a corporate contract negotiated and administered centrally by ICT with the support of Finance. All purchase negotiation, replacement and other matters surrounding mobile phones will be carried out by ICT.
- Changes to configuration or software requests should be sent to the ICT Helpdesk for review and implementation by ICT staff only.
- ICT will define the device type available, referencing the specification of an iPhone 7 or greater.

3.11.3 **Device allocation**

- The user of the mobile phone will be required to confirm receipt via a digital or paper form for the relevant equipment.
- Details of the allocated user and device details will be held within the ICT asset register.
- ICT reserve the right to recall the device if it is identified to be faulty, security risk or if its use is needed continuity.

3.11.4 **Device Accessories**

The purchase of phone accessories is the responsibility of the budget holder to the department to device is allocated. ICT may purchase accessories based on health and safety requirements or for ease of access in line HR guidance.

3.11.5 **Identified Device Usage**

- College Mobile Phones are not to be used for individual “business” or private matters related to personal income generating activities.
- From time to time a personal call may be made, if important. As with the use of other College telephone lines, personal (i.e. non-business) calls should be minimised and where necessary should be of a short duration. This facility should not be abused.

3.11.6 **Call Charges**

- Any private calls that are made, either frequent, long distance, international, or of a long duration may necessitate reimbursement to the College by the user.
- All College phone accounts are monitored, and users shall be responsible for the use and provide an explanation of call charges if requested.
- The cost of business international calls may be charged to the department depending on the reason that the call was made.

3.11.7 **Security of Mobile Devices**

All College mobile devices will be added to the current Mobile Device Management solution where applicable. This gives the College the ability to perform the following actions, but not limited to:

- Configure security policies and restrictions
    - Enforce PIN numbers.
    - Automatically configure applications.
    - Enforce device encryption.
    - Remove primary device features.
- Remotely access and wipe content.
- Remotely lock and unlock the device.
- Remotely track the device if applicable.

Staff issued with a mobile device by the College must ensure the security of the device at all times. The following items should be addressed:

- Should a mobile phone or tablet be lost or stolen, the user must report the matter to ICT within 24 hours, or their next available working day, for notification to service providers and replacement and so that blocks can be put in place to ensure the integrity of any data that may be present.
- Users must care for and use the mobile devices in their possession in a responsible manner. Any damage caused as a result of misuse, lack of care or neglect may result in disciplinary action based on HR protocol.
- Users are required to keep mobile phones clean, and in serviceable condition to the best of their ability and report all irregularities immediately to ICT.
- There are a number of built in protection mechanisms that the user may need during the day to day operation of the mobile phone:
    - Secure the phone at home as if it is a personal possession.
    - Mobile devices must not to be left in unattended vehicles.
    - Whilst at a College site, store the phone and associated equipment with due care. If lending the phone to other members of staff, make a record of when and to whom.

3.11.8 **Procedure for Device Upgrades**

Phone upgrades or replacements must be requested through the ICT Helpdesk. Upon receipt of the request, ICT will deem whether the upgrade is required based on current device operations and job profile requirements. All unused mobile phones should be returned to ICT.

3.11.9 **Use of Personal Mobile Phones**

MidKent College does not undertake to refund any business calls made on personal devices unless prior agreement has been obtained from the

respective budget holder with a justified business case reason to why services provide by the College were not suitable.

To ensure the security of the organisational and personal data that may be held on a user's personal device the College is required to manage a minimum level of security. If a user decides to configure their personal device with the College Microsoft Exchange or through Office365 services, including OneDrive and other Office365 applications, the following settings will be a requirement. If the following settings are not already configured they will be automatically configured as standard:

- The user's device will be encrypted.
- A PIN number will be enforced (this may disable swipe technology on some android phones).

The action of binding a personal device to the College environment means the user agrees to the terms stated above. If the user does not agree with these terms the College email will not be configured on their personal device.

3.12 Virtual Private Network (VPN)

MidKent College employees will be provided access to the College VPN. The required software will be preconfigured on all College devices allowing an Always-On VPN

The following statements identify the terms for VPN usage:

- It is the responsibility of staff to ensure that unauthorised users are not allowed access to the College internal network on their device.
- VPN use is to be controlled by entering your College username and password to authenticate if Single Sign On is not available.
- All internet use, whilst connected via VPN, will be subjected to the filtering and monitoring processes as per 3.11

3.13 Eduroam - Bring Your Own Device (BYOD)

3.13.1 **Terms of BYOD Use**

The Bring Your Own Device network allows all College users and visitors access to the internet whilst they are on-site. Eduroam is a content filtered network and adheres to terms identified in '3.11 Web Content Filtering'.

The College Social Media Policy applies to the Eduroam network. This provides standards expected for appropriate online behaviour, including that between staff and students. It is particularly important to maintain a distinction between personal content and work related content especially when there is interaction that takes place between individuals and where images and content are shared and published.

To ensure our CE+ certification, please be aware that if you connect your personal device to the MidKent College network you may be required to provide evidence around the compliance of your device if it is used to access business data.

3.13.2 BYOD Support

- The College intends to support all devices where possible to access College resources. The ICT Helpdesk should be contacted if users have issues.
- The College takes no responsibility for the maintenance and support of any personal devices.

3.13.3 Incidents and Response

When a security incident, involving a personal device, arises at the College, the College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. The ICT helpdesk will review the incident and decide on the most appropriate and proportionate course of action. The Safeguarding team may be contacted based on the incident. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies. If it is identified that the incident relates to Data Protection, the Data Protection Group will be informed and this will become an investigation run by Data Protection.

4. Duties and Responsibilities

Who is responsible and accountable for each stage of the process:

Section	Title	Responsible Party
3.1	Acceptable Usage Statement	ICT Department
3.2	Information Security & Data Protection	Director of ICT
3.2.1	Approved Storage Locations	Director of ICT
3.2.2	Device Encryption	Director of ICT
3.2.3	Role Based Permissions	Director of ICT
3.2.4	Windows Updates	Director of ICT
3.2.5	Virus & Malware Protection	Director of ICT
3.2.6	Removable Storage Devices	Director of ICT
3.2.7	Accessing College Resources from an Untrusted Source	Director of ICT
3.3	Active Directory Accounts	Director of ICT
3.3.1	Staff Accounts	Director of ICT / HR
3.3.2	Student Accounts	Director of ICT / MIS
3.3.3	Contractors, Consultants & College Affiliates	Director of ICT
3.3.4	Password Policy	Director of ICT
3.4	Printers	ICT Department
3.5	Allocation of Desktop, Laptops and Tablets to Staff	ICT Department
3.6	Laptop & Tablet Trolley/Lockers	ICT Department
3.7	IT Asset Management	Director of ICT
3.8	ICT Purchasing Budgets	Director of ICT
3.9	Waste Electrical and Electronic Equipment (WEEE)	ICT Department
3.10	Web Content Filtering	Director of ICT
3.11	Mobile Phone and Mobile Device Policy	Director of ICT
3.12	Virtual Private Network (VPN)	Director of ICT

3.13	Bring Your Own Device (BYOD)	ICT Department

5. Associated Policies and Procedures

Please see below a list of all associate policies and procedures

- ICT Strategy
- Windows Update Procedure
- Social Media Policy
- Naming Convention Procedure

6 Policy Validity

6.1 This policy is valid for the academic years 2022-2024 and is due for review in October 2024.

7. Policy Owner

7.1 The Senior Manager responsible for this policy is Executive Director for Employers and Corporate Services.

8. Policy Monitoring, Review and Evaluation

8.1 A review of this policy will be undertaken by the review date by the policy writer and will be approved by the Person responsible.

9. Equality Impact Assessment

9.1 This policy has been Equality Impact Assessed and generates no concerns about differential impact. The Equality Impact Assessment is filed on the Quality SharePoint site.