RUNSHAW COLLEGE

POLICY TITLE: IT Access, Usage and Online Safety Policy

APPROVED BY: **Remuneration and Organisational Development Committee**	**AUTHOR**: David Sharrock Approved via SMT FHSE Jan 2017	
POLICY OWNER: David Sharrock	**POSITION:** Director of Facilities	**Version:** 6
LAST UP-DATED: February 2017	**REVIEW DATE:**	
IMPACT ASSESSMENT DATE: January 2017	February 2020	

1.0	**Statement**
1.1	The College recognises the benefits and opportunities which IT offers in both the workplace in general as well as teaching and learning. We actively encourage the use of IT in order to enhance skills, promote achievement and improve productivity.
1.2	We believe that acceptable usage coupled with good online safety practice can be achieved through a combination of security access measures, training, guidance and good practice.
1.3	Effective online safety needs the participation and support of all users of IT facilities and in particular the College's IT facilities. It is the responsibility of every user at college to be aware of this policy and to follow its guidance on the use of all such IT facilities.
1.4	Whilst it is not possible to wholly cater for the use of non-college IT facilities our staff and learners are also expected to behave appropriately whilst using general IT facilities which may have an impact on the College, as an institution, either directly or indirectly or on other members of staff, learners or other users.
1.5	All users are responsible for reporting any known or suspected violation of this policy by another individual or group of individuals.
1.6	The risks associated with the use of IT are compounded by the variety of technologies that are available and the ease of access to resources on the Internet. Whilst the College wants to encourage use of its IT facilities it is equally committed to protecting its staff, learners, partners and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently.
2.0	**Objectives**
2.1	The key objectives of this policy are:

	• To provide guidance on the safe and acceptable use of IT for staff and learners of the College. This includes the use of personal devices (BYODs) to access college resources whilst in college. • To define roles and responsibilities. • To provide guidelines on appropriate action should the policy be breached, or if someone feels the policy may be being breached.
3.0	**Scope**
3.1	The policy applies to all users who have authorised access to the College IT facilities both on the premises and remotely. It also applies to use of IT facilities in general which may have an impact [real or virtual] on the College as an institution or on its staff, learners or governors.
3.2	College IT facilities in whatever format are the property of the College, whether owned or leased. These facilities are only to be used in the interests of the College, its staff and learners, for legitimate purposes.
3.3	Any IT equipment that is loaned to a user is subject to this policy, wherever used.
4.0	**Access - Guidance, Roles and Responsibilities**
4.1	The IT Department are responsible for managing the following: • Staff and learner access to and usage of college IT facilities, services and systems from within and outside college. • Staff and learner access to and usage of college data and associated or derived information from within and outside college. • Guests or visitors when on site.
4.2	College IT facilities include but are not limited to: • Databases. • File Storage (H: G: S: drives etc.) • Email. • Moodle, Portals, remote access. • Configuration of hosts e.g. servers (physical and virtual), switches, security devices, appliances etc. • Logs. • Telecommunication systems. • Hardware. E.g. PCs, Laptops, Macs, Tablets, MFDs and Printers
4.3	Roles and responsibilities are managed by: • Access Control. • Defining what staff/learners can and cannot access. • Defining what staff/learners should and should not [attempt to] do.

	• Defining roles and responsibilities both of owners and IT. • Defining how access is controlled e.g. passwords. • Educating staff and learner regarding access control.
4.4	Monitoring, Audit and Report: • Determining what events will be recorded/logged. • Auditing and monitoring of staff/learner access. • Reporting on individual access. • Decrypt and inspect HTTPS traffic on particular websites such as Google and YouTube to monitor and intercept suspicious searches or activities – this data can be stored and reported to the relevant parties (internal or third party)
4.5	The College provides guidance on: • Staff and learner usage of non-college facilities from within college. • These include, but are not limited to, social media and networking sites, blogs and forums. • Staff and learner usage of non-college facilities from outside college, to access college systems and data i.e. VDI etc. • Management of web presences. • This includes, but is not limited to, web sites, links to the College from other web sites and vice versa, Twitter, Facebook and other social networking sites. • The use of cloud technology. • The creation and use of impersonal, anonymous or generic accounts is strongly discouraged and is at the discretion of the Service Desk. Requests to the Service Desk to create such accounts can only be made by a college manager or authorised staff member via the Service Desk, who will be responsible for all use associated with the account. Advice will be sought on each any request made.
5.0	**Usage - Guidance, Roles and Responsibilities**
5.1	Whilst the College seeks to provide a reasonable level of privacy, data that a user creates on College IT facilities becomes the property of the College. Confidentiality of information stored on college IT facilities is not guaranteed.
5.2	College IT facilities are first and foremost business tools and to assist with the learning experience, and as such, personal use of the system is a privilege and not a right. Reasonable personal use is allowed at certain times and limited to official rest breaks and/or times when they are not on duty (before and after work) for staff. Usage should also have a minimal impact on college resources. Students have access when on college sites as required by their timetable, or in authorised areas in free time. Some college devices may be accompanied by mobile usage plans (including but not limited to iPads, iPhones, etc), in this case strictly no personal use is permitted outside of the UK. Any personal use intended outside of the UK on any college owned device, will require prior SMT approval.

5.3	Any user found to be excessively or inappropriately using the college IT Facilities for non-college related purposes will be subject to disciplinary action. This will also apply in situations where users bring in their own devices such as mobile/smart phones, tablets or laptops and excessive usage occurs during working time.
5.4	The College recognises the occasional need for staff to make or receive short personal calls on college telephones (both fixed line and mobiles), but this privilege must not be abused. It should be noted that calls to mobile telephone numbers are particularly expensive and now form a significant proportion of total call costs. These should be kept to an absolute minimum. Users are normally expected to use their personal mobiles to make personal calls during work or non-work hours.
5.5	Users should not use college IT facilities for: • Personal or private e-mail conversations using their college email address. • Conducting non-college business e.g. personal or private business or buying and selling. • The College may monitor use of college IT facilities at any time for security and network maintenance purposes. College IT facilities may be audited to ensure compliance with this policy.
5.6	Due care must be taken when: • Composing and sending an email message. Emails are legally equivalent to a letter. E-mail messages can be defamatory and can form contracts. For these reasons it is important to take the same care composing e-mail messages as letters. 'All staff 'emails require the prior authorization of a college manager. • The same principles of due care apply to any document or log entry. These documents or logs may be seen by others and in some cases others may have the right to see them. • IT equipment must be treated with care and in accordance with operating instructions. Equipment labelled as "Out of Order" or thought to be unsafe must not be used. Staff should report any equipment with an apparent fault to the Service Desk as soon as possible. Other users should report the fault to a staff member as soon as possible. • Users must not leave their workstation unlocked and unattended. Any user accessing personal data should ensure their display screen is not overlooked by unauthorised persons. Privacy screens can be procured where required via the Service Desk. • Users wishing to physically connect to the College wired network (not Wi-Fi), using personal equipment (BYOD – bring your own device) to college IT facilities would need to be visually inspected, and must consult with and obtain the prior permission of an IT Services staff member. • Any equipment authorised for connection must undergo visual inspection, prior to physical connection. If any personal equipment is suspected of causing degradation to the performance of any college IT facility, IT Services reserves the right to remove it immediately without notifying the owner. The College disclaims responsibility for damage to personal equipment during such disconnection. • Non-staff/learner users are responsible for backing up their own data. College data is backed up regularly and in the event of a system failure IT will attempt to restore data. The College cannot guarantee that data will be restored. There is no means for users to request that files be restored because of accidental erasure. All users should be aware that any data saved anywhere other than on approved college IT facilities is unlikely to be backed up unless special arrangements have been made with IT. • Use of IT facilities is permitted for legitimate purposes and is subject to authorisation.

	The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access to college systems and information. *Legitimate* purposes include legal use in connection with teaching, learning, research and approved business activities of Runshaw College by its staff, learners and other authorised persons. • The College will not tolerate any abuse or unauthorised use of its IT facilities whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the learner and staff disciplinary procedures. • Where conduct is considered illegal, the college will report the matter to the police. The College reserves the right to: o Restrict or suspend any user's access. o Undertake, automatically and one off software monitoring; suspicious activity will be acted upon. o Specifically, under the College's PREVENT and Safeguarding legal duties, automatically use proprietary software to continually monitor all systems (use of wired, WiFi, including BYODs), and issue regular automated reports to authorised parties, both internally and externally if required. o Inspect, copy, remove or alter any data, file, software or system that may undermine the integrity or authorised use of that facility with or without notice to the user. o Monitor and record transmissions made through college IT facilities to ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Telecommunications) 2000 Regulations.
5.7	Every user of college IT facilities should be aware that: • By using college IT facilities, they agree to such monitoring. • The College disclaims responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of college IT facilities. • Use or attempted use of college IT facilities without authorisation may give rise to disciplinary and/or legal proceedings.
5.8	The ability to access a college IT facility, does not imply a right to use that facility or access data. If you have any doubts about which facilities, you are authorised to access you should seek clarification from the Service Desk.
5.9	Under no circumstances are staff or learners authorised to engage in any illegal activity while using college IT facilities. Incitement to commit a crime is itself a criminal offence whether or not the crime is subsequently committed. This includes providing information via computer systems to facilitate crimes. Materials lawful in their place of origin may not be lawful in the UK and *vice versa.*
5.10	It is not possible to produce an exhaustive list of what is allowed or disallowed or of "dos and don'ts" and staff and learners are expected to exercise good judgement during their use of any IT facility. However, some activities are disallowed and staff and learners should not undertake them:

- Using college IT facilities to bully or harass a person [through frequency, language, nature or size] by sending or posting messages of an intimidating, or threatening nature this includes actively or passively engaging in procuring or transmitting material that is in violation of sexual harassment or workplace laws.
- Violation of the rights of any person or organisation protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Unauthorised copying of copyrighted material including digitisation and distribution of photographs from magazines, books or other copyrighted sources, or copyrighted music.
- Executing any form of network monitoring, including port scanning, that will intercept data, unless explicitly authorised to do so.
- Circumventing, or attempting to circumvent confidentiality, data protection, user authentication or security of any system, network or account including accessing or trying to access any user ID or data of another user or attempting to masquerade as another user. Any user who finds a possible security weakness on any college IT facility should report it to the Service Desk, their tutor or an IT facilitator.
- Using any programme/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's computer or denying service to any user via any means, locally or remotely via the Internet/Intranet/Extranet.
- Any form of harassment via e-mail, telephone, texting, instant messaging, social networking or paging, whether through language, frequency, or size of messages.
- College e-mail systems must not be used to transmit unsolicited commercial e-mail or advertising, chain mail, press releases, or other junk mail, except when the user has agreed to receive embedded material within, or is otherwise part of, a service to which the user has subscribed. Users should not use offensive or condescending terms in e-mails or engage in ‘flaming’.
- Users should not procure or acquire ANY software without the prior authorisation of the Service Desk. The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College is strictly prohibited. Only IT have the authority to install or allow installation of software on college IT facilities**.** Any creation or execution of programmes associated with authorised teaching and learning activity is exempt from repeat authorisation requests.
- Any litigation (including fines) resulting from installing unlicensed/illegal software will be paid at the cost of the user.
- The use of images, or photographs where there is a breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or learners. All learners and staff should receive training on the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites, for example.
- IT facilities must not be disassembled or modified. Parts of items must not be removed and disposed of for any reason. Any concerns with IT facilities must be reported to the Service Desk.
- All IT facilities and equipment, whether owned, leased, part of a contract, or free issue, always remain in the ownership of the College.
- Users must take proper care of any loaned equipment and are responsible for its return in proper working order.
- Fair wear and tear is excepted; any loaned equipment which is damaged or lost whilst in the possession of a user will be repaired or replaced at the cost of the user. This extends to the payment of any outstanding lease payments.
- The user is personally liable for any relevant service charges that may arise from the use of the equipment and this may be deducted from my college pay. This includes but is not limited to, any call or data charges which are incurred above and beyond the agreed

	usage plans.
6.0	**Online Safety - Guidance, Roles and Responsibilities**
6.1	Online safety not only covers the obvious, the protection of users from the actions of others, but also the responsibilities of all users to behave in an appropriate manner when using any IT facility. Our aim is to reinforce good practice, as well as offer further information for all users on how to keep their personal information safe and to enjoy using IT safely. To achieve this all users must:
6.2	Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. Users will be held responsible for all actions performed by use of their account.
6.3	IT Services may periodically request users to change their passwords, more frequently than the required programme of 90 days.
6.4	All PCs, laptops and workstations should be secured by logging-off/locking when left unattended.
6.5	The College may automatically append a disclaimer to e-mails sent to external organisations from college e-mail systems.
6.6	Postings from a college e-mail address to newsgroups should contain a disclaimer stating that opinions expressed are strictly the user's own and not necessarily those of the College, unless posting is in the course of authorised college business duties.
6.7	Users must exercise extreme caution when opening e-mail attachments received from unknown senders, or unexpected email attachments received from known contacts, as these may contain viruses or other damaging content. If a user received unsolicited e-mail they should delete it immediately or contact the Service Desk for advice.
6.8	Staff and learners should be aware that data transfer in and out of college is subject to the College Data Protection Policy. Any member of staff or learner that is intending to transfer potentially sensitive data should seek authorisation from the College Data Protection Officer. The use of small portable devices like USB sticks, is considered high risk and are easy to lose.
6.9	No image/photograph can be copied, downloaded, shared or distributed online without permission from the Data Protection Officer and/or SMT. Some teams within the College have prior authorisation due to their roles.
6.10	Photographs of activities on the college premises should be considered carefully and have the consent of the Data Protection Officer and/or SMT before being published. Approved photographs should not include names of individuals.
6.11	All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager.
6.12	When informed about an online safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All users will be advised on what to do if they have online safety concerns

	and who to contact and how to contact them.
6.13	Where any report of an online safety incident is made, all parties will be advised on what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Senior Lead (DSL) may be asked to intervene with appropriate additional support from external agencies.
6.14	The Data Protection Officer(s) (Staff and Learner Officers) and Safeguarding Steering Group, are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents to the DSL and liaising with the local authority and external agencies to promote online safety within the college community.
6.15	Users are responsible for using the College IT facilities and mobile devices in accordance with this policy. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an online safety incident has taken place involving them or another member of the college community. Users must act safely and responsibly at all times when using the Internet and/or mobile technologies.
6.16	All staff are responsible for using the College IT facilities and mobile devices in accordance with this policy, which they must actively promote through embedded good practice. Staff are responsible for attending staff training on online safety and displaying a model example to learners at all times.
6.17	All digital communications must be carried out in line with this policy and be professional in tone and content at all times.
6.18	Online communication with learners is restricted and must only be conducted through • College network/email. • The Virtual Learning Environment (VLE) • Via Social Networking facilities managed by the College. • Via College provided mobiles (Trips and residentials etc.)
7.0	**Data Protection - Personal and Sensitive Information**
7.1	The College collects, stores and processes the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The college will keep that information safe and secure and will use it only as per the agreement with the leaner and within the bounds of the Data Protection Act.
7.2	With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and learners. It is our view therefore, that the college should support staff and learners through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.
7.3	The College has a separate specific Data Protection Policy, all users must be aware of its content and any implications. By using college IT Facilities users are indicating they have read and are fully aware of the contents of the Data Protection Policy.
8.0	**Learners, online safety**

8.1	Online safety applies across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and other emerging technologies. Learners will be advised what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to always cite references properly.
9.0	**Staff, online safety**
9.1	Staff will be expected to set a good example for learners and stakeholders on online safety, by adopting best practice. The Safeguarding Committee will provide guidance to staff in the form of workshops and by providing access to further resources of useful guidance and information.
10.0	**Incidents and Response**
10.1	All incidents are taken seriously. The College will act immediately to prevent, as far as reasonably possible, any damage, harm or further damage or harm occurring.
10.2	Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally.
10.3	Violation of this policy may result in the immediate withdrawal of the user's access to college IT facilities and may further result in disciplinary action and/or legal proceedings.
10.4	All IT facilities and equipment, remains the property of the College, until disposed of via the most appropriate route.
11.0	**Review and Monitoring**
11.1	This policy will be reviewed at least every three years by the Director of Facilities in conjunction with IT Services and the Safeguarding Committee or in line with legislative developments.
12.0	**Related Policies**
12.1	Staff and Governors are also encouraged to refer to other related policies including the Code of Professional Conduct, Data Protection Policy, Print Facilities Policy, Social Media Policy and Health, Safety and wellbeing Policy which are available on Moodle.

A1	**Appendix 1**
	Key Points - Access, Usage and Online Safety
	Users will, where appropriate, be granted access to college-controlled facilities; whilst this access is granted they are expected to adhere to the guidance in this policy. No one should access or attempt to access facilities to which they have not explicitly been authorised or granted access.
	• Users should not access non-college facilities purporting to be representing the College unless this is explicitly authorised by SMT. • Access to college IT facilities are available during college opening hours. Outside such hours – remote access to college facilities such as e-mail, Moodle and portals is provided on a 24 x 7 basis. • Staff are also afforded remote access to documents housed on the college's internal storage servers (E.g. G: H: S: drives) and are expected to exercise the same level of awareness and caution in order to keep this information safe and secure. E.g. Do not leave workstations logged in and unattended, do not share passwords, do NOT use USB drives to house or transport sensitive data. • Should students be provided with the facility to access their H drives remotely in the future, they will be expected to follow the same principles as staff. • User accounts which provide access to facilities are under the control of IT. All staff and learners will have an account (or accounts) which can be used during their period of employment/attendance. • There are some generic accounts which are used in special circumstances. These are under the control of IT and should not be used – unless explicitly directed so. • College IT facilities such as PCs and laptops are provided for the use of staff and can be used to access college and non-college facilities subject to the usage guidance in this document. • College IT facilities such as PCs and laptops are provided for the use of staff and can be used to access college and non-college facilities subject to the usage guidance in this document. • Personal or public devices and facilities should be used with care when accessing college IT facilities. • If a user is absent or unavailable others may be granted access to their files, emails and any other stored data if, in the opinion of management, it is necessary in order to continue operation of the business. • All usage is recorded and may be monitored and reviewed. • Personal use of IT Facilities is a privilege and not a right. Reasonable personal use is allowed where it does not adversely affect the users work and the work of others. Personal use should not occur when users should otherwise be working or undertaking guided learning; Usage has a minimal impact on college resources. • If in doubt, don't! Consult the Service Desk on any issue or concern you may have about

	the use of IT facilities. • If you bring in personal equipment, please consult the Service Desk on whether or not you can use it in college. The exception to this is when the equipment is used solely to access the wireless network. It may also be plugged into a power socket in appropriate areas, as long as you have visually inspected the equipment prior to use. Data should not be copied or transferred from college IT facilities without the express consent of SMT. • The College undertakes software monitoring; suspicious activity will be acted upon. • Usage is limited by volume in a number of instances e.g. amount of e-mail and data storage space. Users should not exceed these limits. • Users should make themselves familiar with and adhere to the College's Social Media Policy. • If in doubt about any situation report it to the Service Desk, Data Protection Officer or a member of SMT. • Never share your account or password.

Appendix 2	
Definitions - The following definitions are used throughout this document	
BYOD	Bring Your Own Device.
college, the College	Runshaw College.
Cloud Storage	The ability to store [and share] files in and across the Internet.
Cloud Technology	IT facilities and resources delivered over the Internet. Included Cloud Storage,
Cyberbullying	Cyberbullying is when one or more people try to tease, harass, threaten or embarrass another person using technology such as mobile phones or the Internet.
Data Protection Officer - Staff and learner	The person or persons responsible for the implementation of the "Principles" of the Data Protection Act. The Data Controller in other parlance.
DSL	Designated Senior Lead - Safeguarding
IT	Information Technology Department.
IT Facility	Any system or service that utilises the College's IT infrastructure including telephones, network, hardware and software.
User	Member of staff, governors, learners, member of the public, visitors accessing college IT facilities.
Safeguarding and PREVENT Committee	Cross-management group at Runshaw responsible for managing and reviewing the College's safeguarding and PREVENT strategy and operation.
Service Desk	The central, single and initial point of contact for all IT related issues.
SMT	Senior Management Team.
Social Media/Social Networking	Technologies which are used to provide interactive dialogue between organizations, communities, and individuals.

Software	Any application or programme, including software that may be designated as demoware, shareware or freeware distributed on [portable] media such as CDs or USB memory sticks as well as that downloaded from the Internet or other file server.