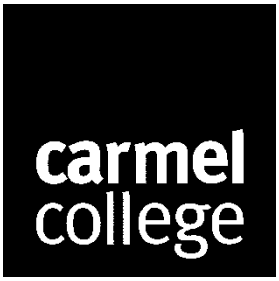

IT and Social Media Acceptable Use Policy for Staff and Students

March 2022

Contents

1. Introduction

1.1. The purpose of this document is to ensure that all users (employees, students, contractors, secondments, visitors etc.) of Carmel College IT Infrastructure are aware of Carmel College policies relating to their use.

1.2. Effective and proper use of information technology is fundamental to the successful and efficient running of Carmel College. However, misuse of information technology - in particular misuse of digital messaging, social media, and access to the Internet - exposes Carmel College to liability and is a drain on time and money.

1.3. Whilst the traditions of academic freedom will be fully respected, it is the responsibility of all users of Carmel College IT Infrastructure to be aware of, and follow all Carmel College IT policies and guidelines and to seek advice in case of doubt. Carmel College's IT policies and guidelines are published on the intranet.

1.4. Carmel College encourages the use of IT Infrastructure for the mutual benefit of Carmel College, its employees and students. The IT Infrastructure is provided to facilitate a person's work as an employee or student of the College, specifically for educational, training, administrative or research purposes. The regulations that constitute this policy seek to provide for the mutual protection of Carmel College and the rights of its employees and students. This policy links to the College **Safeguarding & Child Protection Policy** and the College **Data Protection Policy**.

1.5. Carmel College has attained Cyber Security Essentials certification and must meet these requirements in future.

1.6. For further information regarding safe use of the College's IT Infrastructure please read the **Appendix: e-safety guidance** document.

2. IT Infrastructure

Access to IT Infrastructure is managed by IT Services. Use of any of Carmel College's IT Infrastructure is at the discretion of Carmel College.

2.1. Definitions

2.1.1. The phrase 'IT Infrastructure' as used in this policy is interpreted as including any computer hardware or software owned or operated by Carmel College and any allocation of time, memory, disk space or other measure of space on any of Carmel College's hardware, software, networks or cloud resources.

2.2. Ownership

2.2.1. IT Infrastructure owned by Carmel College and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Carmel College. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

2.3. Desktop PCs

2.3.1. Desktop PCs are a critical asset to Carmel College and must be managed carefully to maintain security, data integrity and efficiency.

2.3.2. Users must consult IT Services if there is a requirement for installing non-standard software on computers managed by IT Services as a Desktop PC.

2.3.3. All users have access to appropriate areas on Carmel College's file servers for the secure storage of valuable files.

2.4. Multi Factor Authentication

2.4.1. All Carmel user accounts will be subject to Multi Factor Authentication (MFA). A suitable device will be needed to perform MFA when accessing college resources when off-site.

2.5. Laptops, tablet and handheld devices

2.5.1. Laptops, tablets and handheld devices are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely.

2.5.2. To protect the integrity of Carmel College systems and data procedures, passwords or authentication devices for gaining remote access to Carmel College systems must not be stored with the computer. This includes the saving of passwords into remote access software.

2.5.3. Highly confidential data should be encrypted to protect it in the event of Laptop PC loss. IT Services can help with this process.

2.5.4. If your Laptop PC or tablet device is lost or stolen IT Services must be notified as soon as possible and a report made to the police.

2.5.5. Handheld and mobiles are at high risk from theft due to their size and nature of usage. Most of these devices have usage tariffs attached to them, loss of the device can expose Carmel College to a large liability through fraudulent use. It is therefore vital that staff are vigilant in caring for their security.

2.5.6. In the event that a device is stolen, staff will be expected to report the theft to the police, obtain an incident number and contact IT Services as soon as possible. IT Services will ensure the mobile service is stopped.

2.5.7. Users of mobile devices must not change technical settings or interfacing configuration with laptops or other equipment without first consulting IT Services. Such changes often cause inadvertently high billing charges or other substantial loss of information or productivity. Staff who alter the configuration of a device so that abnormal billing (or other losses) result, may be liable to compensate Carmel College for any losses.

2.6. Loan Equipment

2.6.1. The policy regarding loan equipment is similar to that for laptops and handheld or mobile devices. Most loan equipment is highly portable and attractive to

thieves. Users who borrow loan equipment should sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.

2.6.2. If loan equipment is stolen or lost, IT Services should be informed immediately. It may also be that the user responsible for its care has to report the theft to the police and report the incident number to IT Services.

2.7. Equipment Disposal

2.7.1. All IT equipment must be disposed of by IT Services using a WEEE certified disposal company. All certificates of disposal shall be kept within IT Services.

2.8. Software

2.8.1. Only software properly purchased and/or approved by IT Services may be used on college hardware. Non-standard or unauthorised software can cause problems with the stability of college computing hardware and it is necessary to contact IT Services if there is a requirement for the installation of such software.

2.8.2. Any additional Software requirement must be approved by IT Services and will be distributed to relevant computers or devices using standardised methods of delivery (System Centre Configuration Manager, Mobile Device Manager etc). IT Services must be consulted prior to any additional/new software being purchased. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.

2.8.3. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, there is always a risk that software could be installed on a machine without the knowledge of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact IT Services who will be happy to assist in resolving any issues.

2.8.4. Non-Standard Mobile Apps loaded onto college owned tablet devices using a personal account are the responsibility of the user in terms of configuration and licencing. IT Services will support Apps on a "best endeavour" basis based on College educational use.

2.9. Additional Systems

2.9.1. Any new or additional system which will interact with existing college IT Infrastructure will only be allowed and configured to do so with the approval of IT Services.

2.9.2. Consultation should be sought with IT Services prior to purchasing any system which will interact with existing college IT Infrastructure, on a basis of interoperability, security and cost.

2.10. Network Access

2.10.1. In order to use the computer facilities of Carmel College a person must first be provided with their own user name by IT services. Registration to use the computer facilities implies, and is conditional upon, acceptance of this **Acceptable Use Policy**. Student usernames will be created automatically at the start of term from the college MIS system. Staff users will be created upon receipt of a "new user" request from the HR Department. All user account will be subject to MFA when accessing college resources off-site.

2.10.2. All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect Carmel College systems from access by unauthorised people: they protect your work and the College's information. MFA provides a second line of defence and blocks unauthorised access to College resources by unauthorised users. The user is personally responsible and accountable for all activities carried out under their username.

2.10.3. The password associated with a particular personal username should be memorised and must not be divulged to another person, except to trusted members of IT services. (The member of IT services will then show you how to re-set your password so that they no longer know it.) Attempts to access, or use, any username, which is not authorised to the user are prohibited.

2.10.4. Passwords must adhere to the following;

i. Be at least ten characters in length;

ii. Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)

iii. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters e.g. not contain "ton" if you happen to be a "burton".

iv. Not be too obvious or easily discoverable;
Mother's Maiden Name
Favourite Pet Name

v. Not contain a Common Password;
Qwerty
Monkey
Princess
Sunshine

vi. The same password should not be used in multiple places, work, personal email, Facebook, Online Banking etc.

vii. If passwords need to be stored for any reason they should be;
Placed in a sealed envelope in a locked drawer / cupboard
Placed in the IT Services or Finance safes
Stored in a secure Cloud Based document with limited access

viii. The use of Password Management software is not encouraged.

ix. Some examples of passwords that will be accepted are...
N@GreenShark2019 (more than 10 characters, Numbers, Capital Letters, Small case letters, Symbols)
#ILikeCheese (more than 10 characters, Capital Letters, Small case letters, Symbols)

PurpleGolfClub12 (more than 10 characters, Capital Letters, Small case letters, Numbers)

2.10.5. Passwords will not expire once set, it is the responsibility of the user to change the password if they think it may have been compromised. The last 24 passwords are remembered and cannot be re-used. Your account will lockout after 10 false attempts, within a 5-minute period. The lockout duration is 15mins.

2.10.6. Carmel College does not allow the wired connection of non-college computer equipment to the network without prior written request and technical approval. The preferred method of remote access is via Remote Destop or VDI systems.

2.10.7. Old student accounts will be disabled during the first term. The accounts will be retained for 2 years in line with the Shibboleth policies. The data files relating to this account will be retained for 1 year as part of the College backup policy.

2.10.8. Old staff accounts will be disabled on the last day of service. It is the responsibility of the staff member to gather any relevant data, files and e-mails they require during their notice period. This data can be copied by IT Services upon request. E-mail can be forwarded to a designated account by IT Services for a period of one term or 3 months. The accounts will be retained for 2 years in line with the Shibboleth policies. The data files relating to this account will be retained for 1 year as part of the College backup policy.

2.11. Wireless Access

2.11.1. Carmel College supplies different levels of wireless access; College Wireless for college owned devices and Guest Wireless (eduroam) for BYOD.

2.11.2. College Wireless is configured on staff laptops and tablet devices by IT Services. Standard logon credentials are used and the laptop or tablet is treated as a wired desktop PC.

2.11.3. Guest Wireless (eduroam) access is open to any wireless client, clients connecting to the Guest wireless will either use their standard Carmel logon credentials, or a guest logon credential. The details of the Guest username and password will be available to all Staff Members, from IT Services, Reception and from the Library desk. By connecting to the Guest wireless users are agreeing to the terms of this document. It is the responsibility of the individual using the Guest wireless to ensure their device is free from viruses and any other malicious software. Access will be only to the Internet and the usual college access controls will be enforced.

2.11.4. For further information regarding the safe use of non-college owned electronic devices please read the **Appendix: “bring your own device” BYOD** document.

3. Data Security

3.1. You must only access information held on Carmel College’s IT Infrastructure if you have been properly authorised to do so and you need the information to carry out your work. It is college policy to store data on a network drive where it is regularly

backed up. Valued documents and files should not be stored on Desktop PCs or laptops. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity. You must ensure that essential data that is not stored on the network file server is regularly backed up.

3.2. Cloud Storage should be used where appropriate and will be protected by MFA when off-site. This includes data stored within email, OneDrive, SharePoint and Teams, the storage of cloud data is managed by Microsoft and has a retention period of 30 days for deleted items so care should be taken when deleting important items.

3.3. Personal data must not be stored on and device either college owned or personal unless sanctioned by IT Services.

3.4. Personal Data and the Data Protection Act

3.4.1. Carmel College maintains a notification with the Information Commissioner's Office in compliance with the General Data Protection Regulations (GDPR) requirements and obligations. This notification is held on a public register and contains details of the College's holding and processing of personal data.

3.4.2. It is the responsibility of all Carmel College staff to ensure that personal data is held and processed within the terms of Carmel College's notification and in compliance with the data protection principles. Carmel College's **Data Protection Policy** outlines the procedures adopted.

3.4.3. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

3.4.4. Do not take "screen shots" or video with your mobile devices of any computer screens that relate to personal data, as this would pose a security risk to that data.

3.5. Freedom of Information Act

3.5.1. Carmel College is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. Employees should be aware that the Act effectively extends rights available under the General Data Protection Regulation to include all types of information held, whether personal or non-personal. Requests will be dealt with according to the Carmel College Policy: Access to Information and Publication Scheme.

3.5.2. Staff should note that all data and correspondence, including digital communication, held by Carmel College may be provided to a data subject, internal or external, in the event of a subject access request.

3.6. Malware Protection

3.6.1. Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Non-Carmel College software or data files intended to be run on college equipment by external people such as engineers or trainers must be

checked for viruses before use. If you suspect that a virus has infected a computer then stop using the computer and contact IT Services immediately.

3.6.2. Files received by or sent by e-mail are checked for viruses automatically. Remote users are responsible for maintaining up to date virus definitions on their own computers and can contact IT Services for help as required.

3.6.3. Users must not intentionally access or transmit computer viruses or similar software.

3.6.4. If any digital communication is received that appears suspect, it must be reported to IT Services as soon as possible.

3.7. Further General Guidance

Carmel College users must ensure prior approval of the Head of IT Services to:

- set-up world wide web sites on Carmel College IT Infrastructure
- publish pages on external world wide web sites containing information relating to Carmel College
- enter into agreements on behalf of themselves or Carmel College via a network or electronic system
- transmit unsolicited commercial or advertising material to other users of a network or to other organisations

4. Digital Communication

4.1. Use and Responsibility

4.1.1. Carmel College's electronic mail (email) system and Teams as a digital communication platform, is provided for the College's business purposes and academic support. Limited personal use of digital communication is permitted, but not to a level that would influence the primary business purpose.

4.1.2. Digital communication is a critical business tool but inappropriate use can expose Carmel College and the user to significant liability. Carmel College, individual members of staff, and students share legal liability for the use of digital communication. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

4.1.3. Carmel College will be held liable for any contractual arrangements entered into by digital communication by members of staff if it is reasonable for the recipient to assume that such people are acting with authority (employer's vicarious liability). Such commitments should be avoided at all costs unless specifically authorised. You should not use your digital communication systems if purchasing personal goods.

4.1.4. The digital communication system costs the college time and money and it must be used judiciously in the same manner as other college resources such as telephones and photocopying. College-wide email messages must be business related and of significant importance to all employees. Non-College email accounts should not be used for conducting College business unless in an emergency situation.

4.1.5. As agreed at the full Governing Body meeting held on 28th March 2017, Board Members may continue to use personal email addresses. Any college business of a confidential nature is to be uploaded to Carmel Connect for Board Members to access and not conveyed via personal email addresses.

4.2. Content

4.2.1. Digital messages must be treated like any other formal written communication. Digital messages cannot be considered to be private, secure or temporary. Digital messages can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

4.2.2. Improper statements in digital communication can give rise to personal liability and liability for Carmel College and can constitute a serious disciplinary matter. Digital communication that embarrass misrepresent or convey an unjust or unfavourable impression of Carmel College or its business affairs, employees, students, suppliers, customers or competitors are not permitted. Do not create or send digital messages that are defamatory. Defamatory digital messages whether internal or external can constitute a published libel and are actionable.

4.2.3. Consider carefully before sending confidential or sensitive information via digital messaging. Digital messages, however confidential or damaging, may have to be disclosed in court proceedings. (Consult IT Services for advice).

4.2.4. Do not create or send digital messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability. It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via digital messaging.

4.2.5. Copyright law applies to digital communication. Do not use digital communication to transmit or circulate copyrighted materials.

4.3. Privacy

4.3.1. Digital messages to or from you cannot be considered to be private or confidential. College digital messages will be regarded as the joint property of Carmel College and the individual member of staff or student.

4.3.2. Although it is not policy to routinely examine the content of individuals digital messages, Carmel College reserves the right to monitor these messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee wrongdoing, protect the rights or property of the College, protect IT system security, investigate serious safeguarding issues, to obtain essential business information after reasonable efforts have been made to contact the user, or to comply with legal process. Digital communications are routinely scanned for the use of offensive language.

4.3.3. Messages sent or received may be copied and disclosed by Carmel College for lawful purposes without prior notice. Requests for access/monitoring unless required by law will only be authorised by the College Principal or Vice Principal.

4.3.4. It is not permissible to access or to send digital messages from another employee's personal account either directly or indirectly, unless you obtain that person's prior written approval.

4.3.5. Members of staff and students will have fixed mailbox sizes. It is expected that staff should effectively manage their email account. Emails fall into five broad functional categories:

- Core business records. These contain information on business transactions, decisions, and discussions to aid that decision. These records are subject to both Freedom of Information and Data Protection legislation.
- Emails containing personal data. These contain information about specific individuals. Subject to the General Data Protection Regulations.
- Personal Reference Records. These are work related emails received or dispatched, and are "of the moment" and will only be relevant for a comparatively short period of time.
- Ephemeral emails. These are work related, but contain information that does not need to be retained as the master document is held elsewhere e.g. circulars etc.
- Personal emails. These are non-work related.

4.3.6. Staff should clear all emails that are no longer current, though those identified as core business records must be filed appropriately. Any emails containing student personal data, for which there is no longer a necessity to retain, must be deleted in accordance with the General Data Protection Regulations. Carmel staff are responsible for storing important documents onto the College network. The IT department can show you how to do this.

5. Internet Usage

5.1. The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities.

5.2. Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited. Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

5.3. Given the impracticality of assessing the exact legal position across all nations, Carmel College Acceptable Use Policy governing material that could be objectionable is grounded in English law, on which basis it is reasonable to expect Carmel College employees and students to have good awareness and to be able to exercise good judgement. If in doubt over a specific case, please discuss with your Curriculum Leader / Line Manager / Tutor.

5.4. Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

5.5. All Internet usage from the Carmel College network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. Audits of sites viewed will be undertaken by IT Services and reported to PATs, and when required to Safeguarding / CMT, as part of the College's response to Safeguarding and the Prevent Strategy. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via Carmel College's Disciplinary Procedure and possibly criminal investigation.

5.6. Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

5.7. Please note that there is no right to access non-work websites and we reserve the right to restrict or remove access to such websites at our absolute discretion.

6. Social Media

6.1. The College internet is provided for the use of the College's official business, but we recognise that many employees and students use the internet for personal purposes, and that many participate in social networking on websites such as Facebook and Twitter. However, all members of the College community are expected to set the highest professional standards at all times, both in and out of College, in order that the College achieves its Mission and that the reputation of the College is safeguarded. This section outlines the responsibilities when using the internet to access social media websites.

6.2. While we respect an employee's right to a private life, we must also ensure that confidentiality and our reputation is protected. We therefore require staff using social networking behave in a professional manner, and do not conduct themselves in a way that is detrimental to the employer. We also recommend that staff create separate social media accounts solely for college use giving clear separation between personal and business accounts.

6.3. All staff must always take care not to allow their interaction on these websites to damage working relationships between other members of staff and stakeholders of Carmel College. Postings to newsgroups social network sites are in effect e-mails published to the world at large and are subject to the same regulations governing digital communication as above. Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Carmel College. For example: "The views expressed are my own and do not necessarily represent the views or policy of my employer." If an employee makes a remark or is responsible for or in any way involved with posting material which in the opinion of the College brings the College into disrepute or otherwise damages the College's interests, disciplinary action may also be taken in line with the College's disciplinary policy. Any legal means may be taken to search accessible materials relating to the disciplinary action.

6.4. Extreme care must be taken if it is necessary to provide endorsements about members of staff, and personal comments about members of staff and students are not acceptable. If in any doubt about other specific usage of site(s) then discuss the matter with your Curriculum Leader/Line Manager or, in the case of students, your tutor.

6.5. Staff must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. In addition, employees should ensure that no information is made available that could provide a person with unauthorised access to the College and/or any confidential information; and refrain from recording any confidential information regarding the College on any social networking website. Care should always be taken to ensure that information provided to such sites does not contravene our **Data Protection Policy**.

6.6. Specific risks associated with social networking are listed via CONNECT through **"Get Safe Online".** They are:

- Disclosure of private information by either yourself or friends/contacts.
- Bullying.
- Cyber-stalking.
- Access to age-inappropriate content.
- Online grooming and child abuse.
- Encountering comments that are violent, sexual, extremist or racist in nature, or offensive activities and hateful attitudes.
- People trying to persuade or harrass you into changing your basic beliefs or ideologies, or adopt an extremist stance.
- Prosecution or recrimination from posting offensive or inappropriate comments.
- Phishing emails allegedly from social networking sites, but actually encouraging you to visit fraudulent or inappropriate websites.
- Friends', other people's and companies' posts encouraging you to link to fraudulent or inappropriate websites.
- People hacking into or hijacking your account or page.
- Viruses or spyware contained within message attachments or photographs.

6.7. "Get Safe Online" offers the following guidelines to avoid these risks:

- Do not let peer pressure or what other people are doing on these sites convince you to do something you are not comfortable with.
- Be wary of publishing any identifying information about yourself – either in your profile or in your posts – such as phone numbers, pictures of your home, workplace or school, your address or birthday.
- Pick a user name that does not include any personal information. For example, "joe_glasgow" or "jane_liverpool" would be bad choices.
- Set up a separate email account to register and receive mail from the site. That way if you want to close down your account/page, you can simply stop using that mail account.
- Use strong passwords.
- Keep your profile closed and allow only your friends to view your profile.
- What goes online stays online. Do not say anything or publish pictures that might later cause you or someone else embarrassment.
- Never post comments that are abusive or may cause offence to either individuals or groups of society.

- Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.
- Always check your account privacy settings to ensure content is accessible to the correct audience.
- Remember that many companies routinely view current or prospective employees' social networking pages, so be careful about what you say, what pictures you post and your profile.
- Don't post your holiday dates - or family photos while you are away - as social networking sites are a favourite research tool for the modern burglar.
- Learn how to use the site properly. Use the privacy features to restrict strangers' access to your profile. Be guarded about who you let join your network.
- Be on your guard against phishing scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.
- If you do get caught up in a scam, make sure you remove any corresponding likes and app permissions from your account.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

6.8. Instant messaging programmes such as texts, i-message, WhatsApp, skype, facetime etc, are free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Care must be taken when using such programmes.

6.9. The College reserves the right to remove access to any social networking site(s) which it feels may inhibit the primary business purpose of College.

6.10. Further information is provided in the **Appendix: Social media for staff guidance** document.

7. Private use, legislation and disciplinary procedures

7.1. Private Use

7.1.1. It Infrastructure is provided for Carmel College's business purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Carmel College.

7.1.2. Carmel College does not accept liability for any personal loss or damage incurred through using the college IT Infrastructure for private use.

7.2. Updates to this Policy

7.2.1. In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

7.3. Relevant Legislation

The following are a list of Acts that apply amongst others to the use of Carmel College It Infrastructure:

Computers' Misuse Act 1990
General Data Protection Regulations 2018
Freedom of Information Act 2000

7.4. Disciplinary and Related Action

As a Beacon College and an Exemplar in the use of IT in education, Carmel College wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its IT users. Examples of behaviour which would require the use of the Carmel College disciplinary actions:

7.4.1. Gross Misconduct examples

Criminal Acts – for example in relation to child pornography
Visiting pornographic sites (e.g. adult top shelf materials).
Harassment – inappropriate e-mails or printed e-mails sent to a colleague/student. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
Obscene racist jokes or remarks which have been shared internally and externally.
Behaviour that could constitute Hate Crime or visiting Extremist sites
Chat rooms – sexual discourse, arrangements for sexual activity
Violation of Carmel College's registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software
Entering into contracts via the Internet that misrepresents Carmel College. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Carmel College is liable for this contract, without first consulting Carmel College's Financial Procedures.
Attempts to break into or damage computer systems or data held thereon e.g. the deliberate introduction of viruses to systems

7.4.2. Misconduct examples

Frivolous use of Company IT Infrastructure that causes annoyance, inconvenience or needless anxiety to others e.g. playing of online or internet games, use of "chat-lines", instant messages, when other students or tutors wish to work on the computers.
Non-academic activities which generate heavy network traffic, especially those which interfere with others legitimate use of IT services.
Downloading and installation of unlicensed products.

This list is not exhaustive, but sets the framework of Carmel College's approach to misuse of IT Infrastructure. Carmel College has the right to monitor employees and students' use of IT Infrastructure where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

In exceptional circumstances, where there are reasonable grounds to suspect that an employee or student has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

File Name/Path	TBC		INTRANET PATH	CONNECT>DEPARTMENTS>COLLEGE POLICIES
Circulation List	Principalship	√	College Union Representatives	
	Full Governing Body		HR Department	
Author/ Responsibility	C Burton Assistant Principal Curriculum		A. Date of Policy approval	
			B. Date next review due	

Carmel College

e-safety Guidance

1. Introduction

Carmel College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the college while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and in light of the Keeping Children Safe in Education 2021 agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety guidance should be read alongside other relevant college policies; Safeguarding & Child Protection and IT Acceptable Use Policy.

2. Creation, Monitoring and Review

The impact of this guidance will be monitored regularly and the guidance will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

3. Scope

This guidance applies to all learners and staff who have access to the college IT systems, both on the premises and remotely. Any user of college IT systems must adhere to and indicate that they have read and accepted the terms of the IT Acceptable Use Policy available at: http://connect.carmel.ac.uk/files/usepolicy.pdf. The e-Safety Guidance applies to all use of the internet and forms of electronic communication such as email, mobile phones and social media sites.

4. Roles and Responsibilities

There are clear lines of responsibility for e-safety within the college. The first point of contact should be IT Services. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All teaching staff are required to deliver e-safety lessons to classes as appropriate and to read through and adhere to the incident reporting procedure as they become aware of any issues. When informed about an e-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 learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be a tutor within college.

Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Safeguarding Lead (DSL) may be asked to intervene with appropriate additional support from external agencies.

Head of IT Services:

The Head of IT Services is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. He/she will be expected to lead the e-Safety Response, complete, review and update the e-Safety Guidance, deliver staff development and training, record incidents, report any developments and incidents to CMT and liaise with the local authority and external agencies to promote e-safety within the college community.

Learner:

Learners are responsible for using the college IT systems and mobile devices in accordance with the college IT Acceptable Use Policy and e-Safety guidance, which they must acknowledge acceptance of. Learners must act safely and responsibly at all times when using the internet and/or mobile technologies. They are responsible for responding to e-safety information and are expected to know and act in line with other relevant college policies e.g. mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the college community.

Staff:

All staff are responsible for using college IT systems and mobile devices in accordance with the college IT Acceptable Use Policy and the e-Safety Guidance, which they must acknowledge acceptance of. Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times and be carried out in line with the college Acceptable Use Policy. Online communication with learners is restricted to the college systems. External platforms not hosted by the college, such as social media sites, may be used following consultation with their Line Manager / Head of Faculty.

This guidance will, however, be monitored and kept under review.
All staff should apply relevant college policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to IT Services and/or line manager without delay. Further information is available on Connect.

5. Security

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 Multi Factor Authentication when off-site, the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of college systems and information, this includes the blocking of USB devices unless encrypted. Digital communications, including email and internet postings, over the college network, may be monitored in line with the IT Acceptable Use Policy. Audits of sites viewed will be undertaken by IT Services and reported to PATs, and when required to Safeguarding / CMT, as part of the College's response to Safeguarding and the Prevent Strategy.

6. Behaviour

Carmel College will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy.

The college will not tolerate any abuse of IT systems. 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 student and staff disciplinary expectations.

Where conduct is found to be unacceptable, the college will deal with the matter internally. Where conduct is considered illegal, the college will report the matter to the police.

7. Communications

Carmel College requires all users of IT to adhere to the College IT Acceptable Usage Policy and Social Media for Staff Guidance. Any extension of this guidance will require express written permission of a member of CMT.

8. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Advice should be sought by tutors / line managers where required.

Carmel College teaching staff will provide information to learners on the appropriate use of images. This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

No image/photograph can be copied, downloaded, shared or distributed online without permission. Photographs of activities on the college premises should be considered carefully and have the consent of the student / subject before being published. Approved photographs should not include names of individuals without consent. This is discussed in the College Data Protection Policy.

9. Personal Information

Personal information is information about a particular living person. Carmel College collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The college will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner/parent/ carer.

No personal information can be posted to the college website unless it is in line with our Data Protection Policy. Only names and work email addresses of staff will appear on the college website no staff or learners' personal information will be available on the website without consent.

For further information see the College Data Protection Policy.

All college mobile devices such as a laptop, USB (containing personal data) require to be encrypted, password protected and a member of IT Services should be consulted before the data leaves the premises.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection Policy.

10. Education and Training

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 stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners:

This guidance will be made available to Learners at the start of the academic year via Connect and PAT sessions.

Issues associated with e-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Learners should also know 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.

For staff:

Further resources of useful guidance and information will be made available to all staff via Connect. Any new or temporary users will receive training on the college IT system as part of their induction. They will also be asked to sign the college Acceptable Use Policy.

Further information is available via a link to "Get Safe Online" when users navigate to the Connect homepage.

11. Incidents and Response

Where an e-safety incident is reported to the college this matter will be dealt with very seriously. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to any tutor or member of staff. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible.

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 depending on the seriousness of the incident. This is in line with the college IT Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

12. Feedback and Further Information

Carmel College welcomes all constructive feedback on this guidance. If you would like further information on e-safety, or wish to send us your comments on our e-Safety approach, then please contact: IT Services – its@carmel.ac.uk

Carmel College
Social Media for Staff Guidance

1. Position Statement

Carmel College recognises the numerous benefits and opportunities which a social media presence offers. The college aims to build relationships and work with the whole community to share news, information and successes. We will endeavour to use social media to engage appropriately with learners, collect feedback to gauge the student learning experience, enhance the college profile within the community and in many ways yet to be discovered.

A social media account provides a flexible delivery platform. The college will use it to supplement our communications but will restrict its use to officially authorised purposes such as communications via Marketing Department and IT Services. The college will actively encourage our staff to make effective and appropriate use of it; to engage in conversations with colleagues and the community as well as sharing appropriate outputs.

In order to provide clarity and consistency for staff, while recognising the corresponding challenges for the college, we have in place procedures to restrict use and some common sense boundaries. Our approach is therefore to support staff to engage with colleagues, learners and the community, while providing appropriate guidance and training on best practice.

Staff are advised to refresh their knowledge of relevant policies which apply in this context, particularly the e-Safety Guidance, IT Acceptable Use Policy and Data Protection Policy. Students may also read this guidance as indicative of the College's approach to social media

2. Authorisation and Review

Any questions relating to this guidance should be addressed to AP Curriculum or IT Services.
The impact of this guidance will be monitored regularly to reflect the changing online environment and technologies. This guidance may also be amended where particular concerns are raised or where an incident has been recorded.

3. Scope

For the purposes of this guidance, social media is defined as any online interactive communication tool which encourages participation and exchanges. Common examples include; Twitter, Facebook, YouTube, Skype, Instagram, Pinterest, WhatsApp, and LinkedIn.

This guidance applies to all staff and to all communications which directly or indirectly, represent the college. It applies to online communications posted at any time and from anywhere, whether to an individual, a limited group or the world.

Carmel College respects privacy and understands that staff may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the institution's reputation are within the scope of this guidance.
Professional responsibilities apply regardless of the medium being used. All social media communications which might affect the college's reputation, whether made either in a private or professional capacity, must comply with relevant college policies which address staff conduct.

Professional communications are those made through official channels, posted on an institutional account or using the college name. All professional communications are within the scope of this guidance (and are subject to the IT Acceptable Use Policy).

Personal communications are those made via a private social media account, such as a personal blog or wiki. In some limited circumstances these communications are subject to this guidance. In all

cases, where a private account is used which clearly identifies the college it must be made clear that the member of staff is not communicating on behalf of the college. An appropriate disclaimer, such as: “the views expressed here are my own and in no way reflect the views of Carmel College”, should be included. Private communications which do not refer to the college, are outside the scope of this guidance.

Staff should refrain from accepting ‘friend’ requests from learners without written line manager approval except where the member of staff has a connection with the learner beyond the context of the institution.

4. Risks, Roles and Responsibilities

There are clear lines of responsibility for social media use within Carmel College.
IT Services is responsible for

- Keeping up to date with technology developments through appropriate CPD
- Reviewing and updating all relevant documentation
- Delivering training and guidance on social media
- Taking a lead role in responding to and investigating any reported incidents
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
- Maintaining a directory of college social media accounts

Staff are responsible for

- Knowing the contents of this guidance and its procedures
- Ensuring that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Informing IT Services where an institutional account is to be used
- Seeking relevant authorisation for official postings prior to publication
- Regularly monitoring, updating and managing content he/she has posted via the college account
- Carrying out an appropriate risk assessment prior to providing access to learners
- Ensuring that all learners have read, understood and agreed to the acceptable use policy, before accessing and posting content via college social media accounts
- Adding an appropriate disclaimer to personal accounts when naming the institution
- Reporting any incidents in line with section 11 below

Line Managers are responsible for

- Addressing concerns or questions regarding posts or comments via official and personal accounts
- Reporting outcomes to IT Services, or escalating the matter to involve appropriate agencies
- Authorising posts, where designated
- Attending additional relevant training

5. Behaviour

Carmel College requires that all staff using social media adhere to the standard of behaviour as set out in this guidance and other relevant policies.

Staff may use social media for the purposes of recruitment selection. Staff will not use social media to infringe on the rights and privacy of colleagues or make ill-considered comments or judgments about staff or the College.

Digital communications by staff must be professional and respectful at all times and in accordance with this guidance. Where an incident is reported, refer to section 11 below. Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the college and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate. The college will take appropriate action when necessary.

Where conduct is found to be unacceptable, the college will deal with the matter internally. Where conduct is considered illegal, the college will report the matter to the police and other relevant external agencies, and may take action according to the Disciplinary Policy.

The use of social media by staff while at work may be monitored, in line with the college monitoring policy.

Carmel College permits reasonable and appropriate access to private social media sites. However, where we suspect excessive use, and consider this use to be interfering with relevant duties, we may take disciplinary action. The following general guidelines apply to staff posting content via social media:

The Do's

- Check with a line manager before publishing content that may have controversial implications for the institution
- Use a disclaimer when expressing personal views which refer to the College
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Manage your social media presence on behalf of the college
- Think before responding to comments and, when in doubt, get a second opinion
- Set up a shadow system i.e. a colleague who can edit or authorise posts
- Seek advice and report any mistakes to your line manager

The Don'ts

- Don't make comments, post content or link to materials that will bring the college into disrepute
- Don't use the college logo/branding on personal accounts
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content given the age and capacity of the learners, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

6. Security

Staff are responsible for ensuring that passwords and other access controls for college social media accounts are of adequate strength and kept secure. Passwords should be regularly changed in line with the college policies and under no circumstances, should passwords be shared. Staff should be familiar with privacy settings and ensure that these are appropriate for both content and intended audience.

Every effort will be made to keep security software up to date. Appropriate security measures will include Multi Factor Authentication when off-site, the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of IT systems and social media accounts. Digital communications, including via social media sites, over the college network, will be monitored in line with the college policies.

7. e-Safety

Carmel College takes e-safety and its duty of care seriously. The college will do all that it reasonably can to ensure that learning and working environments, including online forums, are safe for staff and learners. Whenever a new learning and teaching environment is being considered, staff must consider the information in the e-Safety Guidance document.

8. Use of Other Peoples' Materials

Sharing content such as images, photographs and video is extremely popular and easy to do via social media sites. While this may have value in an educational context, there is a real risk of breaching the rights of individuals who own the different media e.g. images rights, patents, copyright in a blog, or rights associated with collaborative outputs.

All staff should ensure they have permission or other justification to share content in this way. Content is particularly risky where it is commercially valuable, confidential and/or sensitive.

Staff will not post any images, photographs, videos, text etc. via social media sites without appropriate permission from the rights holders. If unsure, staff are advised to check permissions attached to digital content prior to posting via social media.
Further information and guidance is available from IT Services.

9. Personal Information

Personal information is information about a particular living person. No personal information will be shared via social media sites without consent, unless it is in line with our Data Protection Policy. Authorised staff posting content or setting up accounts are responsible for ensuring appropriate informed consents are in place. Members of staff should include their name, email and job title where possible. It is at their discretion whether they wish to post additional contact information.

Staff must keep learners' personal information safe and secure at all times. When using social media sites, staff should only with authority/consent publish learners' or staff members' personal information.

10. Education and Training

Carmel College wishes to make it clear to staff what our guidance contains and the reasons behind it. IT Services will be on hand to answer any queries and address any comments.

11. Incidents and Response

Any breach of this guidance could lead to disciplinary action. Where a breach of this guidance is reported to the college this matter will be dealt with seriously and in line with the college Disciplinary and Acceptable Use policies. The college will act immediately to prevent, as far as reasonably possible, any damage to an individual, their rights or the institution's reputation.

Any stakeholder or member of the public may report an incident to the institution. This should be directed immediately to IT Services or a relevant member of CMT.

Where it appears that a breach has taken place, IT Services or a relevant member of CMT will review what has happened and decide on the most appropriate and proportionate course of action.

Where the incident is considered to be serious, this will be reported to the Principal.
Where staff are in receipt of offensive, unacceptable content via social media, this should be reported to a relevant line manager immediately.

Where questionable content has been received by the institution, IT Services must be informed prior to any response being submitted.

12. Feedback and Further Information

Carmel College welcomes all constructive feedback on this and any other policy. If you would like further information on social media, or wish to send us your comments on our Social Media Guidance, then please contact: IT Services – its@carmel.ac.uk

Carmel College
BYOD Guidance

1. Introduction

This guidance is intended to address the use in the workplace by staff of non-college owned electronic devices such as smart phones, tablets and other such devices to access and store college information, as well as their own. This is commonly known as 'bring your own device' or BYOD. Students may also read this guidance as indicative of the College's approach to BYOD.

It is the policy of Carmel College to place as few technical restrictions as possible on the development and use of new applications and services. However, the use of non-college owned devices to process college information and data creates issues that need to be addressed particularly in the area of data security.

As data controller Carmel must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. As an employee you are required to keep secure college information and data. This applies equally to information held on the college systems and to information held on an employee's own device.

As an employee you are required to assist and support the college in carrying out its legal and operational obligations with regard to college data and information stored on your device. You are required to co-operate with officers of the college when they consider it necessary to access or inspect college data stored on your device.

If you wish to bring your own device and use it to access college data and information (BYOD) you must contact a member of IT Services. The college reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its systems and infrastructure.

2. Security of Systems and Technical Infrastructure

The college takes security very seriously and invests significant resources to protect data and information in its care. The college is contractually required to comply with the Janet Security Policy, to protect the security of Janet and of its own internal networks.

As an employee when you use your own device as a work tool to access the college systems and its data, you are expected to play your part in maintaining the security of college data and information that you handle. This includes security of transfer of data between the personal device and the college system.

This requires that all devices used for storing or processing college data and content have industry standard security passwords in place and that this security mechanism is used to protect that data.

Where a staff member uses their own device to access and store data that relates to Carmel then it is their responsibility to familiarise themselves with the device sufficiently in order to keep the data secure. In practice this means -

- preventing theft and loss of data,
- where appropriate keeping information confidential and
- maintaining the integrity of data and information.

You should –

- delete sensitive or business emails once you have finished with them
- delete copies of attachments to emails such as spread sheets and data sets on mobile devices as soon as you have finished with them

- limit the number of emails and other information that you are syncing to your device.

In the event of a loss or theft, you should change the password to all college services accessed from the devices (and it is recommended this is done for any other services that have been accessed via that device, e.g. social networking sites, online banks, online shops).

In event of loss or theft of a device you should report the matter promptly to IT Services to enable access to college systems by a device or user to be revoked and/or the activation of a remote locate and wipe facility operated by the college. It is recognised that remote wiping of data may result in the loss of the employee's personal information held on the device.

Remote locate and wipe will be used at the discretion of IT Services including where there is a risk that confidential data or personal data has been stored on a device that has been lost, stolen or misplaced.

Certain data should never be stored on a personal device. Any college data that is kept must be stored with the appropriate level of security and in accordance with the college security policy. If you are in any doubt as to the level of security that should attach to particular data then you are required to consult with your manager or IT Services in order to clarify what protection is appropriate. They will be able to provide advice on encryption and approved secure transfer of data.

Failure to comply with this code is considered a disciplinary offence.

3. Security and e-Safety of Staff IT Users

Carmel College is committed to providing a safe environment for learners and staff including the online environment.

Your attention is drawn to the IT Acceptable Use Policy for Staff and Students and to the separate college e-safety guidelines that identifies the role that the college plays in maintaining a safe online working environment. The approach is also summarised in the College Safeguarding & Child Protection Policy.

As an employee you are required to play your part in maintaining a safe working environment and in terms of BYOD this means keeping software up to date and avoiding content that threatens the integrity and security of your device, the college systems and the devices of learners and others. It also means ensuring that the device automatically locks if inactive for a period of time.

The college Social Media Guidelines applies to the BYOD context. This provides standards expected on appropriate online behaviour including between staff and learners. It is particularly important to maintain a distinction between personal content and work related content especially where interaction that takes place between individuals and where images and content are shared and published.

4. Monitoring of User Owned Devices

The college will not monitor the content of user owned devices for threats to the technical infrastructure of the institution. However the college reserves the right to prevent access to the college network by any device that is considered a risk to the network.

In exceptional circumstances the college will require to access college data and information stored on your personal device. In those circumstances every effort will be made to ensure that the college does not access the private information of the individual. College data and information can only be stored and processed on personally owned devices under acceptance of these conditions and with the understanding and agreement of IT Services.

Your attention is drawn to the Acceptable Use Policy which regulates the monitoring of devices used by staff for work purposes. Audits of sites viewed will be undertaken by IT Services and reported to PATs, and when required to CMT, as part of the College's response to Safeguarding and the Prevent Strategy. If certain secure or confidential categories of data and information are required to be

accessed or stored on your own device then Carmel College would be obliged to monitor the device at a level that may harm your privacy and that of anyone you lend your device to. You should consult with IT Services when secure or confidential categories of data are to be handled in this way.

5. Compliance with Data Protection Obligations

The college is committed, as data controller, to treating all personal data fairly and lawfully in line with the General Data Protection Regulations 2018 (GDPR). This includes the requirement to keep personal data up-to-date, and to handle it securely and to keep it for no longer than is necessary

As an employee you are required to comply with the college data protection policy and requirements. Your personal responsibility is expected to align with these college obligations.

Your attention is drawn to the separate Data Protection Policy which requires you as an individual to process data in compliance with all aspects of the Data Protection Act and this applies equally to processing of data which takes place in the context of BYOD.

As an employee you are also required to assist the college in complying with subject access and FOI requests for information and you may be required to search your device and to provide the information requested to the college.

6. Acceptable Use of User Owned Devices

The college requires that employees conduct their online activities which concern the college appropriately and particularly in compliance with the terms of the Acceptable Use Policy (AUP) of the college. This requirement transcends whatever communications technology or device is being used. Our AUP provides guidance on appropriate use of information technology and requires accountability of behaviour by individual staff members. The AUP is available on Connect.

Failure to comply with the Acceptable Use Policy is considered a disciplinary matter.

7. Support

This college intends to support all devices however this may not always be possible and IT Services should be consulted to determine usage levels.

8. Incidents and Response

Where a security incident, involving staff using their own devices, arises at the college this matter will be dealt with very seriously. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. IT Services 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 depending on the seriousness of the incident. This is in line with the college Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

9. Compliance, Sanctions and Disciplinary Matters

Compliance with this guidance forms part of the employee's contract of employment and failure to comply may constitute grounds for action under the college's disciplinary policy.

10. Feedback and Further Information

Carmel welcomes all constructive feedback on this and any other college policy.

If you would like further information on BYOD, or wish to send us your comments on our BYOD Policy, then please contact: IT Services at its@carmel.ac.uk