London
Design &
Engineering
UTC

IT, BYOD and Internet Acceptable Use Policy

Prepared by	Alex Gilchrist, IT Service Delivery Manager, LDE UTC
Acknowledgements	
Date Last Approved	24 November 2022
Policy Approved by	FOA Committee
Version	2.0
Next Policy Review Date	November 2024

Version Control Table

Version	Date	Amended by	Rationale
0.1	19/11/2020		First draft of new policy
1.0	26/11/2020		Version approved by the Committee
1.1	24/11/2022		AGT Review – discourage use of college equipment for personal activity (and setting restrictions), other minor updates and corrections.
2.0	01/12/2022		Version approved by the Committee

Guidance on version Control:
The above is an example of how to complete the Version control table.

Versions are 0.1, 0.2 etc until such point as the document is approved. Then it becomes version 1.0.

Subsequent edited versions become 1.1, 1.2, or if it's a major update, 2.0. Do not worry about the numbers going up and up its about getting the policy right – it's all fine.

IT, BRING YOUR OWN DEVICE (BYOD) AND INTERNET ACCEPTABLE USE POLICY

Policy Coverage

THE POLICY APPLIES OR COVERS THE FOLLOWING GROUPS			
Type of Learner	**Tick (✓)**	**Type of Stakeholder**	**Tick (✓)**
Key Stage 3 (KS3) Carousel	✓	Teaching Staff	✓
Key Stage 4 (KS4) GCSE	✓	Education Support Staff	✓
Key Stage 5 (KS5) Level 2	✓	Administrative Support Staff	✓
Key Stage 5 (KS5) Level 3	✓	Directors	✓
Key Stage 5 (KS5) A Levels	✓	Employers	✓
Apprentices	✓	Visitors / Contractors	✓

Contents

1. Introduction and Policy Aims

IT is an integral part of the way the LDE UTC works, and is a critical resource for learners, staff, Directors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the college.

However, the IT resources and facilities of the college also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of college IT resources for staff, learners, parents and Directors
- Establish clear expectations for the way all members of the college community engage with each other online
- Support the college's policy on data protection, online safety and safeguarding
- Prevent disruption to the college through the misuse, or attempted misuse, of IT systems
- Support the college in teaching learners safe and effective internet and IT use

This policy covers all users of the College's IT facilities, including Directors, staff, learners, volunteers, contractors and visitors.

Breaches of this policy may also be dealt with under the separate Staff Disciplinary Policy.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for colleges

3. Definitions

- **"IT facilities"**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service

- **"Users"**: anyone authorised by the college to use the IT facilities, including Directors, staff, learners, volunteers, contractors and visitors
- **"Personal use"**: any use or activity not directly related to the users' employment, study or purpose
- "**Authorised personnel"**: employees authorised by the college to perform systems administration and/or monitoring of the IT facilities
- **"Materials"**: files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable Use

The following is considered unacceptable use of the college's IT facilities by any member of the college community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the college's IT facilities includes:

- Using the college's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the college's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the college, or risks bringing the college into disrepute
- Sharing confidential information about the college, its learners, or other members of the college community
- Connecting any device to the college's IT network without approval from authorised personnel
- Setting up any software, applications or web services on the college's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the college's IT facilities
- Causing intentional damage to IT facilities
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

- ➢ Using inappropriate or offensive language
- ➢ Using the college's IT facilities to breach intellectual property rights or copyright
- ➢ Promoting a private business, unless that business is directly related to the college
- ➢ Using websites or mechanisms to bypass the college's filtering mechanisms

This is not an exhaustive list. The college reserves the right to amend this list at any time. The leadership team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the college IT facilities.

4.1 Exceptions from unacceptable use

Where the use of college IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the IT or Leadership Teams discretion.

To request access to or use of prohibited equipment/software or websites you must email your request along with full details explaining why and for how long to itteam@ldeutc.co.uk where your request will be processed and approved if appropriate.

4.2 Sanctions

Learners and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the college's policies on learner behaviour or staff conduct.

Users found to be in breach of the IT policy may also be subject to but not limited to the following:

- ▪ Negative behaviour points
- ▪ Internet, email or network block
- ▪ Website and/or equipment restrictions
- ▪ Bandwidth and/or speed restrictions
- ▪ Disciplinary action

The college Behaviour Policy for Learners, which can be found under **Polices** at https://www.ldeutc.co.uk/key-info/.

5. Staff (including Directors, volunteers, and contractors)

5.1 Access to college IT facilities and materials

The IT Team manages access to the college's IT facilities and materials for college staff. That includes, but is not limited to:

- ➢ Computers, tablets, printers and other devices
- ➢ Permissions for software, files & cloud services
- ➢ Network Access

Staff will be provided with a log-in and password that they must use when accessing the college's IT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Team (itteam@ldeutc.co.uk) immediately.

5.1.1 Use of phones and email

The college provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the college has provided.

Staff must not share their personal email addresses with parents and learners and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the IT Team immediately via itteam@ldeutc.co.uk and follow our data breach procedure.

Staff must **not** give their personal phone numbers to parents or learners. Staff **must** use phones provided by the college to conduct **all** work-related business.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use as set out in section 4.

5.2 Personal use

Staff are asked to avoid using college IT facilities for personal use due to the increased risk from cyber threats, if you do use the college equipment for personal use then please be mindful that you are subject to the conditions set out below.

Personal use of IT facilities must not be overused or abused. The IT Team may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during your working hours (excluding lunch breaks)
- Does not constitute 'unacceptable use', as defined in section 4

- You must ensure that you apply the same level of cyber security awareness and care to any personal usage as that of your college work
- Takes place when no learners are present
- Does not interfere with their jobs, or prevent other staff or learners from using the facilities for work or educational purposes
- Will not incur an additional cost to the College which is more than trivial

Staff must not use the college’s IT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the college’s IT facilities for personal use will put personal communications within the scope of the college’s IT cyber security and safeguarding monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) but advised **not** to use such devices to access college work in line with the college BYOD policy.

Staff should be aware that personal use of IT (even when not using college IT facilities) can impact on their employment by, for instance putting personal details in the public domain, where learners and parents could see them.

Staff should take care to follow the college’s guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Social media is not to be used for sharing documents/ collaboration purposes, this must occur through official channels such as the college Office 365 system.

The college has guidelines for staff on appropriate security settings for Facebook accounts (**see Appendix 1**).

5.3 Remote access

We allow staff to access the college’s IT facilities and materials remotely.

The college systems are accessed off-site using two encrypted methods of connection, Remote Desktop Protocol (RDP) and Virtual Private Network (VPN). Staff and Learners are expected to connect via the RDP connection method by following the remote working guidance located in the Staff Area at https://www.ldeutc.co.uk/key-info/.

VPN access is only available to Staff and available upon request. Requests should be submitted to itteam@ldeutc.co.uk, if approved a member of the IT Team will be in touch to install the required software/connection.

Staff accessing the college’s IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the college’s IT facilities outside the college and take such precautions as ensuring that you are connecting via secure network connection and that you only connect using the methods described in the remote working guidance.

You are also required to ensure the device you use to connect to the college is up to date and contains the latest updates to protect against importing viruses or compromising system security.

Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy whilst on-site and off-site.

The college data protection policy can be found under Polices at https://www.ldeutc.co.uk/key-info/

5.4 College social media accounts

The college has an official Facebook (https://www.facebook.com/ldeutc), Twitter (https://twitter.com/ldeutc) and Instagram account (https://www.instagram.com/ldeutc) managed by LDE UTC, Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The college has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

College social media accounts must not be used to share documents unless requested or authorised by the Leadership Team. Social media cannot be used for work collaboration purposes, this must take place on the college learning platform, Office 365.

5.5 Monitoring of college network and use of IT facilities

The college reserves the right to monitor the use of its IT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- All items within College email accounts, including messages sent or received
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised members of the IT Team may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The college monitors IT use in order to:

- Obtain information related to college business
- Investigate compliance with college policies, procedures and standards
- Ensure effective college and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Learners

6.1 Access to IT facilities

IT facilities are available to learners, as follows:

Computers, laptops and equipment within the college are available to learners only under the supervision of staff, devices loaned to learners via the laptop loan scheme can be used both on and off site.

Sixth Form learners can use the computers in the LRC/Fujitsu Hub area independently for educational purposes only, learners from other year groups may be allowed to use these computers with permission of a staff member.

Learners will be provided with an account linked to the college's Office 365 environment (email, OneDrive, Teams etc), which they can access from any device by using the following URL http://portal.office.com and can also use these details to sign in and complete homework set at www.satchelone.com

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the college has the right to search learners' phones, computers or other devices for pornographic images or any other data or items banned under college rules or legislation.

The college can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the college's rules.

6.3 Unacceptable use of IT and the internet outside of college

The college will sanction learners, in line with the Behaviour Policy for Learners (which can be found under **Polices** at https://www.ldeutc.co.uk/key-info/), if a learner engages in any of the following **at any time** (even if they are not on college premises):

Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination

Breaching the college's policies or procedures

Any illegal conduct, or statements which are deemed to be advocating illegal activity

Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

Activity which defames or disparages the college, or risks bringing the college into disrepute

Partaking in activities during lesson time that are not sanctioned by the staff member or college such as playing computer games, using personal devices or watching videos.

Sharing confidential information about the college, other learners, or other members of the college community

Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the college's IT facilities

Causing intentional damage to IT facilities or materials

Using IT or the internet to breach intellectual property rights or copyright

Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

Using inappropriate or offensive language

7. Parents

7.1 Access to IT facilities and materials

Parents do not have access to the college's IT facilities as a matter of course.

However, parents working for, or with, the college in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the college's facilities at the Principals' discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the college online

We believe it is important to model for learners, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the college through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data Security

The college takes steps to protect the security of its computing resources, data and user accounts. However, the college cannot guarantee security. Staff, learners, parents and others who use the college's IT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the college's IT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or learners who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Passwords will be allocated upon first joining the college but are required to be changed upon first sign-on to the college computer. If you are unable to access a computer on-site due to remote learning or working procedures, this requirement will be temporarily rescinded.

8.2 Software updates, firewalls, and anti-virus software

All of the college's IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the college's IT facilities.

Any personal devices using the college's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the college's data protection policy.

The college data protection policy can be found under **Polices** at https://www.ldeutc.co.uk/key-info/

8.4 Access to facilities and materials

All users of the college's IT facilities will have clearly defined access rights to college systems, files and devices.

These access rights are managed by the IT Team.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Team via itteam@ldeutc.co.uk, immediately.

Users must always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The college ensures that its devices and systems have an appropriate level of encryption.

College staff may only use personal devices (including computers and USB drives) to access college data, work remotely, or take personal data (such as learner information) out of college if they have been specifically authorised to do so by the principal.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and password encryption, as defined by the IT Team.

9. Internet Access

The college wireless internet connection is secured and is setup as follows:

- Active Internet filtering to protect against inappropriate websites and/or usage.
- The college Wi-Fi is separated into different areas for Staff, Learners, BYOD and Guests.

Internet filtering is based on block lists and algorithms, whilst this provides excellent protection for our users there are times when websites can slip through the filter. Should you find a website that you feel is inappropriate, malicious or likely to cause serious offence please report the URL immediately to itteam@ldeutc.co.uk.

9.1 Learners

The College provides managed Wi-Fi access to learners.

- Learners can connect to the BYOD SSID
- The connection is encrypted with WPA2 and users are authenticated with our network servers.
- Learners can gain access on their own device by entering their usual College log-in and password.

9.2 Parents and visitors

Parents and visitors to the college are required to request access to the guest Wi-Fi network via reception, this should be arranged in advance by emailing reception@ldeutc.co.uk.

Reception will only grant authorisation if:

- Parents are working with the college in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the college's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must **not** give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Bring Your Own Device (BYOD)

The college understands that using your own device in the workplace brings many benefits and can increase productivity for both staff and learners. To facilitate our users in connecting their personal devices to the network, the college have in place a BYOD network. Due to the nature of connecting your own device to the college network users must be aware of the risks of the devices becoming lost, stolen or compromised in such a way that malicious users can take advantage or you or the college.

10.1 Security

- Personal devices must be up to date with a functioning anti-virus, this includes mobile phones and tablets.
- You must **not** use your personal device to access or create college work due to the increased risk of a security breach occurring
- Devices must be secured with a strong password/pin **and** the device/hard drive encrypted. – **Do not** share your password/pin with **anybody**
- Lock screens must be set to lock after 3-5 minutes of inactivity
- Backup your device using the OneDrive app using your college account, all staff & learners have 1TB of storage each
- Do not allow other people use your device
- Ensure all the security features are enabled, you can do this under "settings" on most devices
- Enable remote wipe and "find my device/phone" if available
- **Never** leave you device unattended and unlocked

10.2 External Use

If you have chosen to use your device on the college network, you must ensure that your device is:

- Only ever connect to secure Wi-Fi and do not use public connections such “free hot spots”
- When not in use, ensure your device is locked at all times whilst on and off-site
- Protect your password/pin when unlocking/logging in your device in a public space

10.3 Staff BYOD Use

Staff are expected to use the laptop provided by the college for teaching and administration work, however personal laptops can be used with prior agreement from either the Principal or IT Team and with the understanding that the college may require security, safeguarding and Mobile Desktop Management software installed and that the college will remotely wipe the laptop if required depending on the security or data risk.

Personal mobile phones, tablets and other devices can be connected by following the BYOD procedures set above without prior approval but it’s use is bound by the guidance, rules and procedures set out within this policy.

Staff who wish to BYOD need to consider what levels of risk using their personal device will bring to the college and if there is a risk of a data breach in regard to the data held/used on their device prior to using them on the system:

Examples of Levels of Risk:

- ➢ High Risk – Special Category data such as racial/ethnic origin, religion, health or financial information.
- ➢ Medium Risk – NI or UPN numbers, names and contact details, unpublished planning/budgeting documentation
- ➢ Low Risk – Publicly available information, college contact details, class handouts, policies and guidance

For further clarification please see the college data protection policy, which can be found under **Polices** at https://www.ldeutc.co.uk/key-info/

Staff must not use their personal device to access or create college work, take photographs or videos of learners, other members of staff or visitors to the college. Photographs and video must only be taken on a college owned device(s) which must be transferred onto the college network after use.

10.4 Learner BYOD Use

Learners are allowed to connect their personal devices as long as they abide by the guidance, rules and procedures set out within this policy.

Learners must not use their personal device to take photographs or videos of other learners, members of staff or visitors to the college. Photographs and video must only be taken on a college owned device(s) with permission of the Leadership Team and must be transferred onto the college network after use by a member of staff.

Learners found running applications (apps) on their personal devices designed to disrupt, damage or compromise the college network will be banned from connecting to the system and face disciplinary action in line with the college Behaviour Policy for Learners, which can be found under **Polices** at https://www.ldeutc.co.uk/key-info/.

11. Monitoring and Review

The LT Team and the IT Team monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the college.

This policy will be reviewed every 2 years.

The governing board via one of its committees is responsible for approving this policy.

12. Related Polices

This policy should be read alongside the college's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

These can be found under **Polices** at https://www.ldeutc.co.uk/key-info/.

Appendix 1: Social Media Guidance Sheet for Staff

Don't accept friend requests from learners on social media

Guidance for College staff personal (non-professional) accounts on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging/identifying other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your learners
6. Don't use social media sites during college hours
7. Don't make comments about your job, your colleagues, our college or your learners online – once it's out there, it's out there
8. Don't associate yourself with the college on your profile (e.g. by setting it as your workplace, or by 'checking in' at a college event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. There have been unconfirmed reports that the app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or learners)

Check your privacy settings (Facebook specific, but similar settings will be available on other Social Media)

- ➢ Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, learners and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- ➢ Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- ➢ The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- ➢ **Google your name** to see what information about you is visible to the public

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A learner adds you on social media

- In the first instance, ignore and delete the request. Block the learner from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the learner asks you about the friend request in person, tell them that you're not allowed to accept friend requests from learners and that if they persist, you'll have to notify senior leadership and/or their parents. If the learner persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the college
  - Learners may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

If you're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current learner or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult with some link to the college, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable Use of the Internet: Agreement for Parents and Carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our college.

The college uses the following channels:

- Our official Facebook, Twitter and Instagram
- Email/text groups for parents (for college announcements and information)
- Our virtual learning platform Office 365 & Satchel One etc

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats.

When communicating with the college via official communication channels, or using private/independent channels to talk about the college, I will:

- Be respectful towards members of staff, and the college, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the college's official channels, so they can be dealt with in line with the college's complaints procedure

I will not:

- Use private groups, the college's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the college can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the college's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other learners. I will contact the college and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 3: Acceptable use agreement for older learners

Acceptable use of the college’s IT facilities and internet: agreement for learners and parents/carers

Name of learner:

When using the college’s IT facilities and accessing the internet in college, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher’s permission
- Use them to break college rules
- Access any inappropriate websites
- Access social networking sites or chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the college’s network using someone else’s details
- Bully other people

I understand that the college will monitor the websites I visit and my use of the college’s IT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the college’s IT systems and internet responsibly.

I understand that the college can discipline me if I do certain unacceptable things online, even if I’m not in college when I do them.

Signed (learner):	**Date:**

Parent/carer agreement: I agree that my child can use the college’s IT systems and internet when appropriately supervised by a member of college staff. I agree to the conditions set out above for learners using the college’s IT systems and internet, and for using personal electronic devices in college, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 4: Acceptable Use Agreement for Staff, Directors, Volunteers and Visitors

Acceptable Use of the College's IT Facilities and the Internet: Agreement for Staff, Directors, Volunteers and Visitors

Name of Staff Member/Director/Volunteer/Visitor:

When using the college's IT facilities and accessing the internet in college, or outside college on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the college's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the college's network
- Share my password with others or log in to the college's network using someone else's details
- Share confidential information about the college, its learners or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the college and with permission of the Principal

I understand that the college will monitor the websites I visit and my use of the college's IT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside college, and keep all data securely stored in accordance with this policy and the college's data protection policy.

I will let the designated safeguarding lead (DSL) and IT manager know if a learner informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the college's IT systems and internet responsibly, and ensure that learners in my care do so too.

Signed (staff member/Director/volunteer/visitor):	**Date:**