Staff Acceptable Use Policy

Embrace Multi Academy Trust strives to maintain and improve good provision and outcomes at each of its member academies. Based upon our shared values and ethos, we aim to support the learning and development of every person within the trust and our policies are written from this perspective.

Signature: ..... Date: .....

Printed Name: ..... Position: .....

Date of Review	August 2021
Next Review	June 2023
Approval By	Trust Leader
Review Frequency	Every 2 years or following required changes

This guidance applies to all teaching and support staff employed within Embrace Multi Academy trust.

1. Scope

- This policy should be followed by all employees of Embrace Multi Academy Trust and individual academies are responsible for ensuring that all employees have read and understand the policy. A summary of the policy is available at Appendix A, which can be signed and returned to individual academy leaders, if this is the preferred method of monitoring within the academy.
- This purpose of the policy is to ensure that all employees have access in their place of work to the internet, email and other technologies in a safe and secure way.
- The policy also extends to out of school facilities eg equipment; printers and consumables; internet and email; virtual learning environments and websites.
- The Acceptable Use Policy also seeks to ensure that employees are not knowingly subject to identity theft and therefore fraud.
- The potential risk to individuals, academies and the trust is such that breaches of this policy could lead to disciplinary action being taken.

2. Equipment

2.1 Vandalism

Vandalism is defined as any action that harms or damages any equipment or data that is part of the trust's/academy's IT facilities and is deemed completely unacceptable. Vandalism is covered by the Computer Misuse Act 1990 (see section 9 - glossary). Vandalism includes, but is not limited to:

- deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware
- change or removal of software (unless this forms part of your role at the trust/academy)
- unauthorised configuration changes (unless this forms part of your role at the trust/academy)
- deliberate deletion of files belonging to other users
- malicious deletion of files created or held by yourself, with the purpose of preventing colleagues or future employees gaining access to material required to undertake their role. (NB: All files created as part of an employee's role, whether on an academy site or not, are the property of the trust/academy. If in doubt about file deletion, please seek advice from the headteacher).

2.2 Use of Removable Storage Media

Embrace Multi Academy Trust accepts that employees may wish to work hours outside of the school day. Where academies have in place a secure and reliable remote access solution, this should be utilised to allow you to continue working from outside of the school, as it ensures that files are stored on the academy network. Where files have to be transported outside of academy premises on removable storage media, **the contents must be encrypted**. Please see section 6.5 for more information on encryption.

2.3 Printers and Consumables

Printers are provided across the trust for use by pupils and members of staff. Printers should be used sparingly and for educational purposes only.

2.3.1 Printer Accounting

The trust reserves the right to monitor printer usage by members of staff. This may be through a printer accounting system or any method that supports the reduction in use of consumables and the reduction of cost.

Printing of whole class resources must be done on larger multi-function printers which are more economical to run than smaller office/classroom-based devices. Under no circumstances should members of staff print off work or homework for pupils.

2.4 Data Security and Retention

If you should accidentally delete a file or files in your folder or shared area, please inform the member of staff responsible for IT services immediately so that attempt at recovery can be made. Recovery may be possible, based upon the system in operation at the trust/academy. Regardless of the system, it is not possible to recover files that were deleted more than two weeks previously.

2.5 Laptop & Tablet Storage

Any trolleys and cabinets provided to ensure mobile devices (laptops and tablets) are safe when not in use, are covered under the terms of insurance. However, all members of staff must adhere to the following guidelines:

- pupils should not be adjacent to the unit when you are unlocking it
- after unlocking the trolley/cabinet always change any padlock code whilst the unit is in use
- never ask a pupil to open a trolley/cabinet for you
- ensure that only members of staff hand out and put devices into the trolley/cabinet
- check devices as they are handed out, and ask the students to check and report any damage at the beginning of the lesson.

2.6 Projectors

Bulbs within classroom projectors have a limited life span, so please use them sparingly. Always ensure you switch projectors off if they are not being used for prolonged periods. Projectors should never be left on during break and lunch times and should always be turned off at the end of the day.

3. Management Information System (Bromcom)

3.1 Communication with Parents/Carers

The MIS system used across the trust allows members of staff to contact parents/carers quickly and efficiently, either one-to-one or in bulk via class or year cohort and has the ability to record this communication directly into the system's communication log.

Whilst this provides the ability to improve communication between each academy and parents/carers, it is essential that this is carried out in a professional manner and according to protocols designed by

each academy. An example of such a protocol is provided at Appendix B and applies to Brockington College. Each academy protocol is the responsibility of individual headteachers. All members of staff must adhere to the guidelines below:

- ensure that the individual academy protocol is followed every time a message is sent to parents/carers from the school MIS
- the individual academy protocol must include that any message being sent to a class-sized cohort or larger, must be approved and proofed by an appropriate member of staff
- only send messages to contacts with parental responsibility
- carefully consider the content of what you are sending, regardless of how many people it is going to. Never send communications in the heat of the moment. Ensure your message is clear and concise and consider how the recipients could interpret the message. It is your responsibility to get communications proofed by a colleague before sending.

3.2 Behaviour Logging

Academies may opt to use the parent portal that provides parents/carers with the ability to view records of their child held by the academy. This may include positive and negative behaviour incidents, which increases transparency within the school and increases dialogue between the academy, parents/carers and pupils. If this is the case, it is essential to consider the content of all behaviour logs.

Negative Behaviour Incidents:

To save confusion over what is and is not appropriate to share with parents, and to avoid any potential issues surrounding GDPR (sharing other pupils' names etc.) **under no circumstance should the comment box be filled in for negative behaviour incidents.**

If you wish to note a comment next to an incident please log this as an 'Internal Comment' as these are only accessible within school.

Any member of staff found in breach of this instruction could be subject to the school disciplinary procedures. As such, please exercise caution and diligence when logging incidents.

Positive Behaviour Incidents:

Comments are encouraged when recording positive behaviour incidents. This allows parents/carers to receive individual, personalised feedback on their child's positive behaviour within school.

Under no circumstances should other pupils be named or mentioned within comments that are accessible to parents/carers.

4. Internet and Email

4.1 Content Filtering

The trust provides internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any

inappropriate website or content whilst using IT equipment, **you must report it to a member of the IT team or the academy headteacher immediately.**

4.2 Acceptable Use of the Internet

All internet access is logged and actively monitored. Please be aware that computer usage reports (internet history) can and will be provided to senior leaders upon request. Use of the internet should be in accordance with the following guidelines:

- only access suitable material – the internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law
- do not access internet chat sites, unless directly work related. Remember you could be placing yourself at risk
- never give or enter your personal information on a website, especially your home address, your mobile number or passwords
- do not access online gaming sites, unless they have an educational relevance. Remember that your use of the internet is for educational purposes only
- do not download or install software from the internet, as it is considered to be vandalism of the trust's/academy's IT facilities
- do not use the internet to order personal goods or services from online, e-commerce or auction sites
- do not subscribe to any non-educational newsletter, catalogue or other form of correspondence via the internet
- do not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

4.3 Email

You will be provided with an email address by the trust/academy and the expectation is that you will use this facility for legitimate educational and administrative activity.

You are expected to use email in a responsible manner. Sending or receiving messages which contain any material that is of a sexist, racist, unethical or illegal nature or is likely to cause offence must not take place. All email sent through the trust/academy email system must be work-related and personal email should not be used during the school day.

When sending an email, remember to:

- use appropriate and professional language
- do not reveal any personal information about yourself or anyone else. Remember that electronic mail is not guaranteed to be private
- consider the file size of an attachment
- do not download or open file attachments unless you are certain of both their content and origin
- never have Outlook open when using your projector or interactive whiteboard.

The work email account you are provided with, and its contents, remain the property of Embrace Multi Academy Trust at all times and should only ever be used for school purposes not private emails. As

with all data held on the system, senior leaders reserve the right to access any information held without any prior warning. A search of any emails relating to a child or parent/carer can be requested under Subject Access Requests and the Freedom of Information Act (see Section 5.7) and we have a legal obligation to provide this.

As with all computer misuse, inappropriate use of the email systems is a disciplinary issue and will be subject to the trust's disciplinary guidelines.

Section 4: External Services

4.1 Web-Email

Web-email provides remote access to your email account from home or anywhere with an internet connection. Where the trust/academy makes this service available, it is subject to the following guidelines. Use of the facility will be closely and actively monitored.

- web-email, where provided, is for the use of members of staff and pupils only. Access by any other person is not allowed
- never reveal your password to anyone
- remember to treat file attachments with caution. File attachments may contain viruses that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Embrace Multi Academy Trust accepts no responsibility for damage caused to any external equipment or software, as a result, of using a web-email service.

4.2 Virtual Learning Environment (VLE) Software

VLE (eg Moodle) provides a web-based portal allowing users access to personalised learning resources and lesson materials. Where this service is provided at an academy, it should be used in accordance with the following guidelines:

- the VLE is provided for the use of Embrace Multi Academy Trust staff and pupils only. Access by any other party is strictly prohibited
- never reveal your password to anyone or attempt to access the service using another user's login details.

4.3 Social Networking Websites (Facebook, Twitter, Instagram etc)

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of your professional reputation and that of the trust/academy when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. This policy is in place to assist staff to:

Maintain reasonable standards in their own behaviour that enable them to maintain an effective learning environment and also to uphold public trust and confidence in the profession.

GTCE Code of Conduct 2009

Please find below the guidance from the Safer Recruitment Consortium:

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and avoid any communication which could be interpreted as 'grooming behaviour'.

Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web-based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable.

Staff should adhere to their establishment's policies, including those with regard to communication with parents and carers and the information they share when using the internet

Guidance for safer working practice for those working with children and young people in education settings. Safer Recruitment Consortium, May 2019

As such the trust policy for social networking sites is as follows:

- social media sites must be used in a professional manner and any information placed in the public domain must be carefully considered and not contain any personal information. For details on setting security permissions on social networks please see a member of the IT support team or the academy headteacher
- all information uploaded must be carefully considered and under no circumstances bring the trust/academy into disrepute
- staff members must not make 'friends' or interact online with current or former pupils under the age of 18 using any social networking sites. This includes gaming on the internet using websites, apps or game consoles. If you feel that there is a valid reason for contact with current or former pupils in this manner, you MUST discuss the matter with the academy headteacher and gain written/email consent
- it is advisable not to add former pupils over the age of 18 to your friends list to maintain maximum professional distance
- the trust recommends that staff using social networking sites restrict contact with parents and carers of current and former pupils to those with whom they have a personal friendship.

4.4 Using Social Media within the Academy (Twitter)

As a trust, we appreciate that the use of social media is increasing and can be a great tool to provide information and resources to parents/carers and pupils using tools they are already familiar with and are using on a daily basis.

As such we are happy for academies to use Twitter as a learning tool, but have the following guidelines relating to its use:

- to comply with Twitter terms of service, as well as retaining accountability for posting, it is important for people posting to Twitter to have their own unique username and password which is **not shared with others**. This means that either:
    - a single academy or departmental twitter account is created which a single member of staff is responsible for (eg @BC-English)
    - members of staff within a department have their own twitter accounts and passwords (eg @BC-English-MrS)
- all communication must remain **professional and transparent** at all times. To that end:
    - all topics must be related to your academy or subject area and things that are going on in and around the school at all times
    - any form of private messaging whether it is to pupils, parents/carers or colleagues is strictly prohibited
    - the account should be used for posting content only. Accounts should not be used to follow/subscribe to parent/carer and/or pupil feeds
    - retweeting of other users' accounts and articles should be carefully considered and be relevant and specific to your subject area
    - all content posted must be carefully considered and anything which could be misinterpreted, misconstrued or otherwise bring the trust into disrepute, must be avoided
- inform the headteacher (all academies other than Brockington College) or the IT Team (Brockington College only) of all Twitter accounts being created so they can be monitored and promoted via the website/academy social media as necessary.
- read the 'Twitter Rules' to ensure you comply with their terms of service: https://support.twitter.com/articles/18311#

4.5 Uploading Video Content

Videos can be recorded and added onto the learning platforms used by academies to provide a more personalised, varied and unique selection of learning resources. When doing so it is important to follow the guidelines below:

- ensure that the environment you are presenting from is clear from personal effects and is a professional representation of the school at all times
- when recording videos, please consider GDPR. The means ensuring any work shared cannot be personally identified, and students must not be individually named
- think carefully about the content being shared and ensure that it is professional and could not bring the school into disrepute
- videos generally turn out best in a brightly lit environment without a strong source of light in the background. If possible place the recording device on a tripod and/or flat surface for a more professional video
- if staff have any queries regarding what is or is not acceptable to be posted, please contact the academy headteacher or IT Support Team (for Brockington College staff) who can advise further.

4.6 Live Lesson Streaming (Broadcast)

- only use a medium for broadcasting eg Google Classrooms to conduct live lessons with students for which the school has completed a Data Protection Impact Assessment (DPIA). If in doubt, check with the academy headteacher or IT Support Team (for Brockington College staff)
- all live lessons must be attended by two members of staff
- at the beginning of the lesson remind students about personal privacy and to ensure the camera is disabled and microphone muted using the buttons on the main screen
- if using screen-sharing please bear in mind that it is possible your laptop screen will be shared with all participants. Due to this please:
    - ensure that only appropriate content is shared
    - sign in to any external websites necessary for demonstration purposes before starting the session to ensure your username and password are not divulged.
- you must wait for all students to leave the classroom before exiting yourself. Failure to do this will leave the classroom open and students can remain in the room
- ensure that the environment you are presenting from is clear from personal effects and is a professional representation of the school at all times.

5. Privacy and Data Protection

5.1 Passwords

- never share your password with anyone else or ask others for their password
- when choosing a password try to use a selection of the following: uppercase letters | lowercase letters | numbers | special characters
- a good example of a secure password may use numbers to replace letters such as Br0ck1ngt0N.
- if you forget your password, inform a member of the IT department or the academy headteacher immediately
- if you believe that someone else may have discovered your password, then change it immediately and inform a member of the IT team or the academy headteacher.

5.2 Security

- never attempt to access files or programs to which you have not been granted access. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.
- always lock your computer (CTRL+ALT+DEL) when away from your desk, whether for 30 seconds or an hour
- you must report any security concerns immediately to the headteacher (all academies other than Brockington College) or the IT team (Brockington College only). If you are identified as a security risk to the academy's IT facilities you will be denied access to the systems.

5.3 Bromcom

All workstations intended for staff use have a link to the Bromcom Management Information System installed. Although access to what information is displayed is restricted based on user level access,

having Bromcom open increases the risk of pupils accessing sensitive information. Please follow the guidelines below when using the Bromcom system:

- ensure that your password to access Bromcom is both secure (see Section 5.1) and different to your network password
- always ensure your projector is switched off before opening Bromcom
- never leave your computer unlocked with Bromcom open, always CTRL+ALT+DEL before leaving your desk.

5.4 Projector Data Security Considerations

Please follow the guidelines below when using the projector within your classroom:

- the projector should only be used when presenting information to the class, not left on all day
- the projector must be frozen/turned off before opening up any application which could potentially contain confidential information. This includes, but is not limited to, Bromcom, email and the staff shared area
- it is your responsibility to ensure that any sensitive data remains secure and that the Data Protection Act is not breached.

5.5 Storage and Safe Transfer of Secure Data (Encryption)

Some academies have put in place a secure, encrypted remote access solution which is the preferred method for working off-site and/or outside of the school day. Should confidential files (anything with identifying information on – pupil names, grades etc) need to be taken off-site on physical media then the files must be encrypted, either using a hardware encrypted device or using software encryption such as VeraCrypt. Please speak to a member of the IT team if you need more information on this. Any staff laptops used to take sensitive information off-site must also be encrypted using Bitlocker and have a secure password (see Section 5.1).

5.6 Disposal of Secure Data

All computers which have had access to sensitive data are disposed of in a secure manner and to Government (Ministry? of Defence) standards.

5.7 Freedom of Information Act

Under the Freedom of Information Act (2000) academies must disclose, if asked to do so, any information which is requested by a member of the public unless there is a good legal reason not to.

For members of staff, this means that any information, including electronic information, which includes information about a child, whether formal (grade books, reports etc) or informal (email communications) can be requested at any time and each academy has a legal obligation to provide it.

5.8 Data Protection Act (Including the General Data Protection Regulation) 2018

Under the Data Protection Act you are personally accountable in ensuring that data you have access to is kept in a secure manner and is not shared or otherwise accessed by anyone other than yourself. This includes:

- ensuring information is not shared with third-parties unless a Data Processing Agreement is in place approved by the data protection officer
- ensuring that access to your account is secure and you do not share your password with anyone else
- as you are personally accountable under GDPR for any data breach, remote access should be used at all times to access confidential data. If materials are taken off-site they must be securely encrypted (please see section 5.5 of this policy).

6. Monitoring pupil use of IT facilities

It is expected that all members of staff will monitor pupils' use of IT facilities and ensure they are using them acceptably and responsibly whilst under the staff member's supervision. This includes, if necessary and where available, using AB Tutor to monitor student activity. Training for AB Tutor is available on request from the IT Support Team.

Key points to note are as follows:

- pupils should only be using IT resources for educational purposes during lesson time and access to online games is not allowed. This is outlined clearly in the pupil acceptable use policy and if pupils are found accessing games whilst they should be working, they will be subject to the same consequence system that would be applied for any other behavioural issue. Please apply the academy behaviour policy before requesting internet or emails bans, which are issued for serious breaches
- academies may choose to have a policy around the withdrawal of ICT facilities from pupils following serious breaches
- pupils should only use email for educational purposes and at times agreed by the teacher. They should not be sending any other emails during lesson time
- pupils should not be intentionally trying to bypass the academy's filtering system and attempting to access inappropriate material. Any student found doing so should be reported to the headteacher (all academies other than Brockington College) or via itsupport@brockington.leics.sch.uk (Brockington College) immediately.

7. Service

Whilst every effort is made to ensure that the systems, both hardware and software, are working correctly, the trust or individual academies will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages may include loss of data as a result of delay, non-deliveries, missed deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via each academy's IT system is at your own risk. Embrace Multi Academy Trust specifically denies any responsibility for the accuracy of information obtained whilst using the IT systems.

8. Health and safety

- when using projectors please ensure you do not look directly into the projector bulb
- ensure no food or drink is near any IT equipment

- report any faulty equipment or wiring to the academy headteacher/ IT team as soon as possible.
- be careful when wheeling laptop trolleys around. Ensure there is no-one in the way and push the trolley rather than pulling it for greater control and to see where you are going.

9. Glossary

Computer Misuse Act

The Computer Misuse Act makes it an offence for anyone to have:

- unauthorised access to computer material, eg if you find or guess a fellow colleague's password and use it
- unauthorised access to deliberately commit an unlawful act, eg if you guess a fellow colleague's password and access their learning account without permission
- unauthorised changes to computer material, eg if you change the desk-top set up on your computer or introduce a virus deliberately to the academy's network system.

Data Protection Act (2018)

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone across the trust, including teaching staff, support staff, volunteers and governors.

The act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in each academy. The act not only applies to paper files, it also applies to electronic files.

The principles of the act state that data must:

- be fairly and lawfully processed
- be processed for limited purposes
- be adequate, relevant and not excessive
- be accurate and up to date
- be kept no longer than necessary
- be processed in accordance with data subject's rights
- be secure
- not be transferred to other countries without adequate provision.

RIPA – Regulation of Investigatory Powers Act 2000

If a request for authorised access is made to any academy they will provide the appropriate access to your IT records and files. The act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

- the interception of communications
- the acquisition and disclosure of data relating to communications
- the carrying out of surveillance
- the use of covert human intelligence sources

- access to electronic data protected by encryption or passwords

If a request for authorised access is made to any academy, we will provide the appropriate access to your IT records and files.

Freedom of Information Act (2000)

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities; and. members of the public are entitled to request information from public authorities.

Should any academy receive a request, it will be processed in accordance with the act.

Appendix A: Staff acceptable use policy summary

Please find below a summary of the main areas covered within the Staff Acceptable Use Policy. Please note that it does not replace the full document. This form can be used as signed acceptance of the policy.

- Access to the internet and email is provided to assist in carrying out your job. These functions should only ever be used for work related tasks. Use of these functions should not be considered private and internet histories and/or email logs can be requested at any time, so please remain professional and courteous at all times
- Whilst the projector or interactive whiteboard is a useful resource for conveying information to children it is essential that it is used carefully and responsibly so that pupils cannot see or access any confidential information. Under no circumstances should email or Bromcom be opened whilst projecting information to your class
- It is your responsibility to ensure that any confidential information which you have been given access to is used responsibly and only for its intended purpose. Under no circumstance should any confidential information leave the trust/academy unless properly encrypted (please see the academy headteacher/a member of the IT support team if you are unsure how to do this). Failure to comply with this is not only a breach of the policy but also the Data Protection Act
- It is your responsibility to monitor pupil use of IT facilities. Whilst we put in place systems and precautions to protect pupils from inappropriate material online, no system is 100% accurate and should you suspect pupils are accessing something they should not be accessing, you must report it to the IT support team (Brockington College) or headteacher (all academies other than Brockington College) immediately
- Your use of social media (Facebook, Twitter etc) outside of school should remain professional at all times. Please uphold standards that would be considered appropriate to your profession and do not bring your academy or the trust into disrepute
- The Freedom of Information Act allows anybody for whom the trust/academy holds information about to request release of such information, no matter what form it is in. In short, this means that parents/carers and pupils over a certain age can at any point request any information relating to them or their child, both formal (grades, medical information etc) and informal (notes, email communication) and we have a legal obligation to provide it. Please take note of this when you record information
- Behaviour incidents must be logged in line with this policy. IMPORTANT: never log parentally accessible comments (labelled 'comment' within Bromcom) alongside negative behaviours.

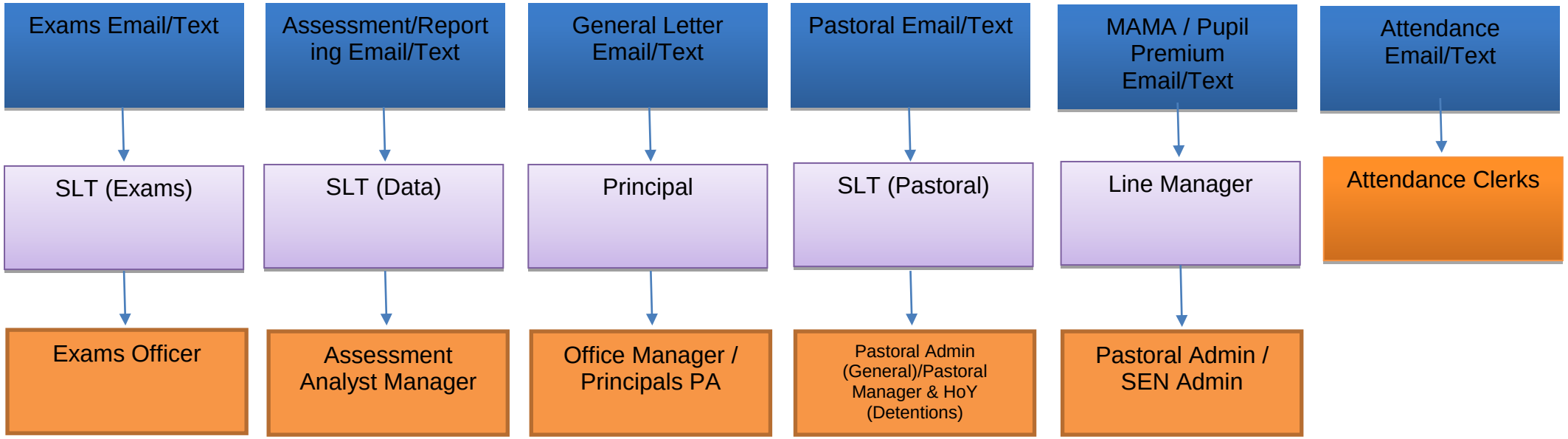
I have read and understood the trust Acceptable Use Policy, and I am signing below to confirm my acceptance of the conditions of use contained within it.

Name: _____

Signature: _____

Date: _____

Appendix B: Example Communications Flow Chart (In use at Brockington College)



Person Proofing Text / Email

- Ensure spelling and grammar is correct
- Ensure message remains professional
- Ensure the correct communication method (text/email has been selected)
- Ensure text/email targets the correct audience
- If text message, ensure it meets character limits (160) and is prefixed with BC:

Person Sending Text / Email

- Ensure message has been proof read according to chart
- Ensure correct group has been selected