Acceptable Use Policy

Policy lead:	**Director of People**
Last review date:	31 August 2022
Next review date:	31 August 2024
Approval needed by:	**Finance and Staffing Committee**

History of most recent policy changes

Date	Page / Section	Change	Origin of change e.g. Legislation, TU request
01 December 2020	Whole document	Change to The Learning Alliance	Merger into new organisation
31 August 2022	New section	EIA	Reflect good practice

Policy Equality Impact Screening

Date of screening: **31 August 2022**						
Name of person completing screening:						
	Does this policy have the potential to impact on people in any of the identified groups?		What is the expected impact of this policy on any of the identified groups			Notes
	Yes	**No**	**Positive**	**Neutral**	**Negative**	
Age						
Disability						
Gender Reassignment						
Race or Ethnicity						
Religion or Belief						
Marriage						
Pregnancy/ Maternity						
Sex						
Sexual Orientation						
Should the policy have a Full Equalities Impact Assessment? **Yes**/**No**						

Carrying out personal activities
Staff must not carry out personal activities during working hours or mix private business with official duties. Trust equipment and materials should not be used for private purposes. This applies to all employees (as a contractual term), agency staff and to individuals acting in a similar capacity to an employee. It applies to staff of contractors and other individuals providing services/support to the Trust (e.g. volunteers).

This applies to:
• mail systems (internal and external)
• internet and web based services (email, cloud technology and video conferencing)
• telephones (hard wired and mobile)
• pagers
• fax equipment
• computers
• photocopying, printing and reproduction equipment
• recording / playback equipment
• accessing or producing documents and publications (any type or format)

Compliance
When using Trust equipment all staff should comply with, as relevant, Financial Regulations and Codes of Practice on Financial Management, terms of employment, including the Code of Conduct for Employees and other Trust policies. It is not acceptable to use the Trust's equipment and materials to do any of the following:
• Activities for private gain, for example freelance work or private business use
• Illegal activity
• Gambling
• Political comment or any campaigning
• Harassment or bullying
• Accessing sites or using words/images which could be regarded as sexually explicit, pornographic or otherwise distasteful or offensive
• Insulting, offensive, malicious or defamatory messages or behaviour including those that are racist or sexist or any other conduct or messages which contravene employment or diversity policies
• Actions which could embarrass the Trust or bring it into disrepute
• Personal shopping
• Excessive personal messages
• Personal communications to the media that have not been authorised by the Trust
• Using message encryption or anonymised web search, except where encryption is required for official business purposes
• Loading software or documents from the internet not agreed with the Trust

If an employee inadvertently accesses an inappropriate web site using Trust equipment, they should close it immediately and notify a Network Manager of the incident, giving the date and time, web address (or general description) of site and the action taken.

The Network Manager will produce a half termly report of all incidents for the Headteacher's consideration. Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take any action within their authorised power to safeguard or resolve the situation (e.g. disconnect any infected machine from the network (remove the cable)) and notify the Network Manager.

Monitoring, surveillance and security
Monitoring information will not be accessible (or distributed) any more widely than is necessary for the purposes for which it is needed.

All employees should be aware that, in relation to any electronic communication, there can be no expectation of absolute privacy when using the Trust's equipment provided for official / work purposes; and that the Trust reserves the right to monitor all communications including their content. This monitoring is carried out to

ensure that equipment and systems are used efficiently and effectively, to maintain systems securely and to detect any breaches of this policy or the law.

Surveillance cameras are installed by the Trust only for security and safety reasons and will always be visible to people within their range. Recordings will be kept secure and the information used for security purposes only. No automatic connections will be made between information from security cameras and other monitoring sources.

Every employee must observe the communications and information technology security requirements and act responsibly when using equipment and materials. The Trust will take the most serious view of any action or inaction on the part of an employee who deliberately, recklessly or carelessly jeopardises the security of records or systems. This includes employees leaving laptops or computers in cars, unattended at the Trust and allowing students to use their computer using their access rights.

Reporting Misuse
If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately. Breaches of this, or any breach of the above, may result in the application of the Disciplinary Procedure and may, if deemed sufficiently serious, be treated as gross misconduct, which may lead to dismissal.

In the case of contractors, agency staff, volunteers or partnership employees, breach may result in termination of the contract or relevant arrangement and/or withdrawal of the relevant facility. Reports will be made to the Local Authority Designated Officer if it is believed that the misuse has the potential to become a safeguarding issue. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

Using email, text messages and social media
All staff are issued with a work email address and are expected to check their email at the start of each day. If staff experience difficulty using email, they should report this to the network manager. Emails sent outside of working hours should not expect a response until the next working day. Email should be composed with the same professional levels of language and content as applied for any other public written letters or other media. Remember that email is not a substitute for face-to-face communication, where that is possible, and that any email can be misconstrued however well worded. Similarly, remember to ask the question of 'who needs to receive this email?' before pressing 'send' or 'reply all'.

Staff should not use a personal email address for work business, and nor should they divulge their personal email address, or personal mobile telephone number, to students or correspond with students or parents using it. If they are sent an email by a student to their personal account, then they should report this to a senior colleague.

The Trust recognises that many employees make use of social media in a personal capacity. Any communications that employees make in a personal capacity through social media must not bring the Trust into disrepute, breach confidentiality, abuse their position of trust when working with children/young people, breach copyright or do anything that could be considered discriminatory against, or bullying or harassment of, an individual. Staff must not correspond with students using personal social media accounts. They must not accept friend requests from current students using personal accounts. Staff should not use photographs taken legitimately in school on their personal social media site(s).

Data Protection Email Guidance

1. Is an email necessary? A conversation may be better if possible.
2. All school email usage must be in line with the Acceptable Use Policy.
3. Language and tone should be appropriate and professional at all at times.

4. Use initials in emails as far as possible and avoid the use of individuals' names.
5. Do not send, reply or forward emails to more people than is necessary, especially when there are attachments on the original email. Avoid 'reply all' and 'forward all'.
6. Proofread before sending.
7. Always double-check the recipient's email address is correct.
8. Do not use email as a storage device or archive by making sure that unnecessary items are regularly deleted from email folders.
9. Confidential information should never be sent within the body of the email but attached within a separate encrypted document, marked CONFIDENTIAL in the subject header and a received request included.
10. Do not leave your emails visible on your own mobile or home devices screens when not in school.

Related Document: Staff Code of Conduct
Social Media Policy

It is expected that this policy is read on an annual basis and staff indicate this has been actioned.