THE LEARNING ALLIANCE

Code of Conduct

Policy lead:	**Janet Robinson**
Last review date:	1 December 2020
Next review date:	1 December 2021
Approval needed by:	**Finance and Staffing Committee**

All employees have a responsibility to act and to take decisions based on public interest and should act with honesty, integrity, objectivity and impartiality at all times. They must always act in accordance with the trust that the community and everyone within it is entitled to place on them and be open about, and take accountability for, their actions and decisions. Everyone has a right to be treated with fairness and equity and all employees must ensure that they always comply with the Trust's policies, and the law, relating to equality and discrimination.

In order to safeguard both the Trust and its staff from charges of misconduct or malpractice, it is important that staff are aware of the standards of conduct they are expected to observe. This Code of Conduct reflects the reasonable behaviour expected of all employees as professionals. Employees also need to take care that their behaviour outside the workplace does not conflict with their work responsibilities and will not bring the individual school or Trust into disrepute. Any infringement of this or any related Code may be dealt with as a disciplinary matter.

RELATIONSHIPS

Employees at The Learning Alliance are expected to:

- demonstrate consistently high standards of personal and professional conduct
- maintain high standards of ethics and behaviour, within and outside school
- treat others with dignity,
- build relationships, rooted in mutual respect
- observe proper boundaries with students by establishing and maintaining appropriate professional boundaries and standards with children regardless of culture, disability, gender, language, racial origin, religious belief and/or sexual identity
- demonstrate respect for diversity and promote equality
- show tolerance of and respect for the rights of others.

ATTENDANCE & PUNCTUALITY

Staff are expected to maintain high standards in their own attendance and punctuality. Staff should be aware of the contents of the Trust's Absence and Attendance Management Policy available on the website.

SAFEGUARDING

Staff are expected to have regard for the need to safeguard students' well-being, in accordance with statutory provisions and the Trust's safeguarding arrangements. Staff should complete Safeguarding training and refresh this knowledge every 3 years as part of the school's on-going INSET programme. They should ensure they have read:

- Guidance for Safer Working Practice for Adults who work with Children and Young People.
- Guidance for Safer Working Practices for Adults who Work with Children and Young People (School Summary)
- Safeguarding Policy for Children and Young People

RECRUITMENT

Employees who are involved in the recruitment and selection process should follow the Trust's policies on recruitment and selection and should ensure that all appointments are made on merit. It is unlawful for an appointment which is based on anything other than the ability of the candidate to do the job required. Recruitment and Selection processes place a wide range of employees in a position where they may be able to influence decisions. Employees involved in the process must ensure that candidates

are selected on their ability to do the job required. Employees should not be involved in any appointment where they are related to, or have a close personal relationship with any of the applicants. This also includes providing a reference

CAR USE

If you use your car for school business you will need to provide the Finance Department with evidence of your car insurance, driving licence and log book. If you are taking children in your car as part of an organised activity, then this should be risk assessed and authorised in advance through Evolve, with prior agreement by parents, and in line with the Visits Policy. You should not give lifts to students on their own in your car unless in extreme circumstances, and in such an event you must try to notify the school as soon as practically possible.

HEALTH & SAFETY

Staff should maintain the highest standards of health and safety and have regard for their own Faculty or Key Area expectations and requirements – e.g. ADT, Science, P.E., Site Maintenance.

APPROPRIATE USE OF ICT FACILITIES

See Appendix 1 : Acceptable Use Policy below.

GDPR

Staff are expected to comply with all aspects of the General Data Protection Regulations and to follow the policy as set out in the Data Protection Policy. Key aspects of Data Protection will be included in Inductions and updates provided at least annually as part of the INSET training programme.

DRESS CODE

Staff will wish to dress in a manner consistent with their professional status, acting as role models for students and promoting confidence in the Trust. Staff should dress according to the Dress Code.

DISCLOSURE OF INTERESTS AND MEMBERSHIPS

Employees must disclose to the Director of Finance and Governance any financial or non-financial interest they or their spouse have, whether direct or indirect, in any contract, company, other public body or any other matter that involves or may involve the Trust.

HOSPITALITY

Hospitality is likely to be acceptable where it is clear that the invitation is corporate rather than personal. All offers of hospitality must be authorised in advance by the Chief Executive, Chief Operating Officer or Chair of Trustees.

GIFTS

Employees should not accept personal gifts, other than those which could be considered as small tokens or gestures. For further information or advice on this please contact the Director of Human Resources or Director of Finance and Governance.

ADDITIONAL PAID WORK

If you have another job it must not be allowed to affect your work within the Trust or official responsibilities. If you feel there is any impediment to your role at the Trust, then you should disclose this to the Headteacher.

INTELLECTUAL PROPERTY

Anything invented or created as part of your job (i.e. in the course of normal duties or in the course of duties falling outside normal duties, but specifically assigned to you, and the circumstances in either case were such that an invention might reasonably be expected to result in the carrying out of your duties) is described as "intellectual property" and normally belongs to the Trust. You should not exploit this to your own advantage or for any financial gain.

WHISTLEBLOWING / CONFIDENTIAL REPORTING

If you know or suspect someone is breaking this code or acting wrongly, you are positively encouraged to raise your concerns with the Headteacher, Executive Principal, Director of Human Resources or a Governor. More detail is provided in the Confidential Reporting (Whistleblowing) Policy.

Useful Links:

Data Protection Policy
Disciplinary Policy and Procedure
Dignity at Work Policy
Dress Code
Equality and Diversity Policy
Recruitment Policy
Staff Handbook

Appendix 1

Acceptable Use Policy

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).

Acceptable Use applies to the use of:

- 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 the ICT Network Manager of the incident, giving the date and time, web address (or general description) of site and the action taken. The ICT Network Manager will produce a half termly report of all incidents for SLT'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 ICT 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 Headteacher 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 ICT network manager. 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). (See **Social Media Policy** – Appendix 2 below)

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.

Appendix 2

Social Media Policy

AIMS

To support all employees by establishing clear guidelines on the proper use of social media so that:

- the Trust is not exposed to legal challenge;
- the reputation of the Trust is not adversely affected;
- employees do not put themselves in a vulnerable position;
- employees understand how information provided via social networking applications can be representative of the Trust; and
- the use of social media does not impact on the Trust.

PRINCIPLES

The Trust recognises that many employees make use of social media in a personal capacity and, in most cases, this is uncomplicated and trouble-free. Whilst the Trust respects an employee's right to a private life and has no wish to interfere with this, when using such sites employees must consider the potential impact it could have on their professional position, their own reputation and that of the Trust. The following identifies how an employee's personal life and work life can start to overlap.

- By identifying themselves as employees of the Trust, i.e. adding the Trust name on profiles, the perception of users will be that staff are representative of the Trust. It is therefore important that employees are mindful of the professional standards that are expected of them. Anything posted, including innocent remarks, have the potential to escalate into something that could potentially damage the image and reputation of the Trust, or undermine its work. The originating comment may be traced back to an employee of the Trust and, even if they have not been involved in the latter stages of the comments, they may find themselves subject to a disciplinary investigation.

- Individuals making complaints search the web for information about staff involved in their case – finding social networking sites, blogs and photo galleries that could give fuel to their concerns or help them to identify personal information about them.

- Journalists increasingly use the web to research stories, and may reprint photos or comments that they find.

- Law firms research social networking sites as a matter of course in preparing divorce, private law children's cases and other court proceedings.

- Some organisations also look on social networking sites to find out information about people applying for jobs.

SOCIAL MEDIA

Definition of social media

For the purpose of this policy, social media is any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. The term social media refers to a number of online networking platforms such as:

- blogs (written, video, podcasts), e.g. WordPress, Blogger, Tumblr;
- micro-blogging websites, e.g. Twitter;
- social networks, e.g. Facebook, LinkedIn;
- forums/message boards;
- online dating sites, e.g. Tinder, Grindr; and
- content-sharing sites, e.g. Flickr, YouTube and Instagram.

Employees should be aware that there are many more examples of social media and this is a constantly changing area. Employees should follow the guidelines outlined in this policy in relation to any social media that they use.

Personal use of social media at work

Employees are not allowed to access social media websites for their personal use from the Trust's computers or devices at any time. This includes laptop/palm-top/hand-held computers or devices (e.g. mobile phones) distributed by the Trust for work purposes.

The Trust understands that employees may wish to use their own computers or devices, such as laptops and palm-top and hand-held devices, to access social media websites while they are at work. However, in accordance with the Trust ’s current rules and regulations contained in the Staff Handbook, employees are not allowed to access such devices (e.g. mobile phones) for private purposes during working hours (unless there is an emergency). Such devices should always be switched off and stored in a safe place during contact time.

Social media in a personal capacity

The Trust recognises that many employees make use of social media in a personal capacity. However, the employee's online profile, e.g. the name of a blog or a Twitter name, must not contain the Trust's name. Furthermore, while they are not acting on behalf of the Trust, employees must be aware that they can damage the Trust if they are recognised as being one of the Trust’s employees. Any communications that employees make in a personal capacity through social media must not:

a. bring the Trust into disrepute, for example by:
    - criticising the Trust;
    - criticising or arguing with management, colleagues, children or their families;
    - making defamatory comments about individuals or other organisations; or
    - posting images that are inappropriate, for example, photographs of themselves or colleagues taken at work or links to inappropriate content;

b. breach confidentiality, for example by:

- revealing any information owned by the Trust; or
- giving away confidential information about an individual (such as a colleague or child) or an organisation, e.g. the Trust or the Local Authority;

c. abuse their position of trust when working with children/young people, for example by:
   - contacting children or their families through social networking sites unless the reason for this contact has been clearly and firmly established by the headteacher, executive principal or chair of governors;
   - accepting any requests to become a named friend on a social networking site made by a child/young person; or
   - uploading any photographs or video containing images of children/young people for whom the employee holds a position of trust unless in line with the Trust procedures;

d. breach copyright, for example by:
   - using someone else's images or written content without permission;
   - failing to give acknowledgement where permission has been given to reproduce something; or

e. do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
   - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
   - using social media to bully another individual (such as an employee of the Trust);
   - using social media to exclude other individuals; or
   - posting images that are discriminatory or offensive.

Security and identity theft

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private. Employees should never send abusive or defamatory messages.

Employees 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. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:

- ensure that no information is made available, or referred to, that could provide a person with unauthorised access to the Trust and/or any confidential information;
- inform their manager immediately if they suspect that their personal site has been compromised or accessed by an unauthorised person;
- refrain from recording any confidential information regarding the Trust on any social networking website;
- check their security settings on social networking site so that information is only visible to the people who they want to see it;
- put their name into an internet search engine to see what people can find out about them; and
- help friends and colleagues out by letting them know if they spot things on their pages that might be misconstrued.

Defamatory statements

Material posted on a site may be defamatory if it contains something about the Trust's employees, partners, children or other individuals that an employee may come into contact with during the course of their work that is not true and undermines the Trust's reputation. For example, photographs or cartoons that may have been doctored to associate the Trust or its employees with a discreditable act.

Libellous statements

Material posted on a site may be considered libellous if it is in permanent form and directly or indirectly clearly identifies the Trust or one of its employees or children with material that damages their reputation. Employees should always use their own judgment but should bear in mind:

- that information that they share through social networking sites is still subject to copyright, Data Protection, Freedom of Information and Safeguarding legislation;
- the Code of Conduct; and
- other relevant Trust policies (e.g. Dignity at Work, Whistleblowing Procedure, Equality Policy and policies and guidance regarding acceptable use of email, intranet and internet whilst at work).

DISCIPLINARY ACTION

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action under the Trust's disciplinary procedure. In situations where it becomes known that an employee has posted material to be defamatory or a breach of contract, the employee will be asked to remove the offending material from the social media site immediately.

Serious breaches of this policy, e.g. incidents of bullying of colleagues or social media activity causing serious damage to the Trust, may constitute gross misconduct and could result in dismissal.

MONITORING

Data relating to the operation of this policy will be collated and monitored regularly to ensure that the policy is operating fairly, consistently and effectively. Issues that are identified from the data will be dealt with appropriately.

This policy applies to The Learning Alliance employees only, does not form part of an employee's terms and conditions of employment and is not intended to have contractual effect. However, it does set out current practice and policy and employees are strongly advised to familiarise themselves with its content. The policy will be reviewed in the light of operating experience and/or changes in legislation.