Code of Conduct

Policy lead:	**Director of Human Resources**
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
31 August 2022	Whole document	Revised content	To reflect changes to KCSiE
23 January 2023	Whole Document	To reflect synchronicity across all key safeguarding policies.	As part of strategic work on QA of safeguarding 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**						

Commented [MEH1]: This screening is not complete?

This policy refers to all adults (staff, visitors, governors, clubs, sports coaches). All adults 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. Employees who believe that other employees may be breaching this Code of Conduct have a duty to report this, in confidence, to the Head Teacher and/ or line manager who will investigate the situation and, where necessary, take appropriate action. Employees who report a potential breach of the code will not be penalised or discriminated against for having done so. Please access the following link: WHISTLEBLOWING POLICY. The Trust expects volunteers, governors and Trustees to also act with personal and professional integrity, respecting the safety and wellbeing of others.

GENERAL OBLIGATIONS

Staff set an example to pupils. They will:

- Maintain high standards in their attendance and punctuality
- Never use inappropriate or offensive language in school
- Treat pupils and others with dignity and respect
- Show tolerance and respect for the rights of others
- Not undermine fundamental British values, including democracy, the rule of law, individual liberty, and mutual respect and tolerance of those with different faiths and beliefs
- Not express personal beliefs in a way that exploits pupils' vulnerability or might lead them to break the law
- Understand the statutory frameworks they must act within
- Adhere to the Teachers' Standards

SAFEGUARDING

Staff have a duty to safeguard pupils from harm, and to report any concerns they have. This includes physical, emotional and sexual abuse, and neglect.

Staff will familiarise themselves with their individual school's 'Child Protection and Safeguarding Policy' and associated procedures, including the Prevent initiative, and ensure they are aware of the processes to follow if they have concerns about a child.

Schools' 'Child Protection and Safeguarding Policy' and associated procedures are available in the documents section of the payroll system, on the policies section on the school's website and from the DSL within each school. New staff will also be given copies as part of the induction process.

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:

- KCSIE: Guidance for Safer Working Practice for Adults who work with Children and Young People.
- KCSIE: Guidance for Safer Working Practices for Adults who Work with Children and Young People (School Summary)
- The school's Safeguarding Policy for Children and Young People

Allegations that may meet the harm threshold

This section applies to all cases in which it is alleged that anyone working in the school, including a supply teacher, volunteer or contractor, has:

- Behaved in a way that has harmed a child, or may have harmed a child, and/or
- Possibly committed a criminal offence against or related to a child, and/or
- Behaved towards a child or children in a way that indicates they may pose a risk of harm to children, and/or
- Behaved or may have behaved in a way that indicates they may not be suitable to work with children – this includes behaviour taking place inside or outside of school

These can include incidents outside of school which do not involve children but could have an impact on their suitability to work with children.

Any concerns of this nature, about the conduct of other adults, should be taken to the Headteacher without delay or, where that is a concern about the Headteacher, to the Chair of Governors and the LADO. Staff should be aware that this must be done on the same working day. We will deal with any such allegation quickly and in a fair and consistent way that provides effective child protection while also supporting the individual who is the subject of the allegation. We will report instances to the LADO and follow their recommendations.

A 'case manager' will lead any investigation. This will be the headteacher (or delegated representative), or the chair of governors where the headteacher is the subject of the allegation.

We make all staff aware of their duty to raise concerns. Where a staff member feels unable to raise an issue or feels that their genuine concerns are not being addressed, other whistleblowing channels may be open to them.

As part of our whole Trust approach to safeguarding we promote an open and transparent culture in which all concerns about adults working in or on behalf of The Learning Alliance (including supply teachers, volunteers and contractors) are dealt with promptly and appropriately. This includes allegations which do not meet the harms threshold, also known as low level concerns.

Low-level concerns about members of staff

A low-level concern is a behaviour towards a child by a member of staff that does not meet the harm threshold, is inconsistent with the staff code of conduct, and may be as simple as causing a sense of unease or a 'nagging doubt'. For example, this may include:

- Being over-friendly with children
- Having favourites
- Taking photographs of children on a personal device
- Engaging in 1-to-1 activities where they can't easily be seen
- Humiliating pupils

Low-level concerns can include inappropriate conduct inside and outside of work.
Low level concerns will be reported in the same way as a concern in relation to concerns and allegations that meet the harms test i.e. to the Headteacher (Mrs Caroline Lowe) or Chair of Governors (Mr Neil McKinlay), if the concern is about the headteacher. We also encourage staff to self-refer if they find themselves in a situation that could be misinterpreted. If staff are not sure whether behaviour would be deemed a low-level concern, we encourage staff to report it.

All reports will be handled in a responsive, sensitive and proportionate way. Unprofessional behaviour will be addressed, and the staff member supported to correct it, at an early stage.

This creates and embeds a culture of openness, trust and transparency in which our values and expected behaviour are constantly lived, monitored and reinforced by all staff, while minimising the risk of abuse.

Records of low-level concerns will be reviewed so that potential patterns of concerning, problematic or inappropriate behaviour can be identified and responded to.

Where a pattern of behaviour is identified, the Head will decide on a course of action. This might be internal disciplinary procedures, or referral to the LADO if the harms threshold is met.

The Head will consider if there are any wider cultural issues in school that enabled the behaviour to occur and if appropriate policies could be revised or extra training delivered to minimise the risk of recurrence.

Whistle-blowing
Whistle-blowing reports wrongdoing that it is "in the public interest" to report. Examples linked to safeguarding include:

- Pupils' or staff's health and safety being put in danger
- Failure to comply with a legal obligation or statutory requirement
- Attempts to cover up the above, or any other wrongdoing in the public interest

Staff are encouraged to report suspected wrongdoing as soon as possible. Their concerns will be taken seriously and investigated, and their confidentiality will be respected.

Staff should consider the examples above when deciding whether their concern is of a whistle-blowing nature. Consider whether the incident(s) was illegal, breached statutory or school procedures, put people in danger or was an attempt to cover any such activity up.

Staff should report their concern to the headteacher. If the concern is about the headteacher, or it is believed they may be involved in the wrongdoing in some way, the staff member should report their concern to the Chief Executive or chair of the governing board.

Concerns should be made in writing wherever possible. They should include names of those committing wrongdoing, dates, places and as much evidence and context as possible. Staff raising a concern should also include details of any personal interest in the matter.

For our school's detailed whistle-blowing process, please refer to our 'Whistle-blowing Policy'.

STAFF-PUPIL RELATIONSHIPS
Staff will observe proper boundaries with pupils that are appropriate to their professional position. They will act in a fair and transparent way that would not lead anyone to reasonably assume they are not doing so.

If staff members and pupils must spend time on a one-to-one basis, staff will ensure that:

- This takes place in a public place that others can access
- Others can see in to the room
- A colleague or line manager knows this is taking place

Staff should avoid contact with pupils outside of school hours if possible.

Personal contact details should not be exchanged between staff and pupils. This includes social media profiles.

While we are aware many pupils and their parents may wish to give gifts to staff, for example, at the end of the school year, gifts from staff to pupils are not acceptable.

If a staff member is concerned at any point that an interaction between themselves and a pupil may be misinterpreted, or if a staff member is concerned at any point about a fellow staff member and a pupil, this should be reported in line with the procedures set out in our child protection and safeguarding policy.

COMMUNICATION AND SOCIAL MEDIA
School staff's social media profiles should not be available to pupils. If they have a personal profile on social media sites, they should not use their full name, as pupils may be able to find them. Staff should consider using a first and middle name instead, and set public profiles to private.

Staff should not attempt to contact pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find pupils' or parents' social media profiles.

Staff will ensure that they do not post any images online that identify children who are pupils at the school without their consent.

Staff should be aware of the Trust's Social Media and Acceptable Use Policies (Appendices 1 & 2).

ACCEPTABLE USE OF TECHNOLOGY
Staff will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

Staff will not use personal mobile phones and laptops, or school equipment for personal use, in school hours or in front of pupils. They will also not use personal mobile phones or cameras to take pictures of pupils.

We have the right to monitor emails and internet use on the school IT system. See Acceptable Use Policy - Appendix 1 below.

CONFIDENTIALITY
In the course of their role, members of staff are often privy to sensitive and confidential information about the school, staff, pupils and their parents.

This information should never be:

- Disclosed to anyone unless required by law or with consent from the relevant party or parties
- Used to humiliate, embarrass or blackmail others
- Used for a purpose other than what it was collected and intended for

This does not overrule staff's duty to report child protection concerns to the appropriate channel where staff believe a child has been harmed or is at risk of harm, as detailed further in our child protection and safeguarding policy.

HONESTY AND INTEGRITY
Staff should maintain high standards of honesty and integrity in their role. This includes when dealing with pupils, handling money, claiming expenses and using school property and facilities.

Staff will not accept bribes. Gifts that are worth more than [amount] must be declared and recorded on the gifts and hospitality register.

Commented [MEH2]: This needs to be agreed or taken out?

Staff will ensure that all information given to the school is correct. This should include:

- Background information (including any past or current investigations/cautions related to conduct outside of school)
- Qualifications
- Professional experience

Where there are any updates to the information provided to the school, the member of staff will advise the school as such as soon as reasonably practicable. Consideration will then be given to the nature and circumstances of the matter and whether this may have an impact on the member of staff's employment.

DRESS CODE
Staff will dress in a professional, appropriate manner. Each school has their own set of guidelines setting out their expected 'dress code'. Staff are asked to read and understand this document.

CONDUCT OUTSIDE OF WORK
Staff will not act in a way that would bring the school, or the teaching profession, into disrepute. This covers conduct including but not limited to relevant criminal offences, such as violence or sexual misconduct, as well as negative comments about the school on social media.

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 Attendance Management Policy available on the website.

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.

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.

DISCLOSURE OF INTERESTS AND MEMBERSHIPS

Employees must disclose to the Trust 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 Chief Operating Officer.

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 the job (i.e. in the course of normal duties or in the course of duties falling outside normal duties, but specifically assigned to the employee, and the circumstances in

either case were such that an invention might reasonably be expected to result in the carrying out of their duties) is described as “intellectual property” and normally belongs to the Trust. The employee should not exploit this to their own advantage or for any financial gain.

Useful Links:
- Data Protection Policy
- Disciplinary Policy and Procedure
- Dignity at Work Policy
- Dress Code
- Equality and Diversity Policy
- Management of Attendance Policy
- Recruitment Policy
- Whistleblowing Policy

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

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 school or 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 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 school 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). (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, TikTok;
- 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. Employees should also be aware that content uploaded to social media is not private. Even if you restrict access to friends, there is still the capacity for it to be re-posted and distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect. Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the school/trust's social media accounts.

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, 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.

EQUALITY
The Learning Alliance will ensure that, when implementing this policy, no employee will be disadvantaged on the basis of their gender or transgender, marital status or civil partnership, racial group, religion or belief, sexual orientation, age, disability, pregnancy or maternity, social or economic status or caring responsibility. This means that the guidelines may need to be adjusted to cater for the specific needs of an individual including the provision of information in alternative formats where necessary.

REVIEW
The policy will be reviewed in the light of operating experience and/or changes in legislation.

Related Policies:
Disciplinary Policy and Procedure
Dignity at Work