



CHELMSFORD
LEARNING
PARTNERSHIP

CODE OF CONDUCT

Certain expectations for good conduct are described in specific Trust policies and procedures and professional expectations are set out in national and local conditions of service and in the national 'Teacher Standards'. This policy supplements these provisions and provides additional guidance for adults working in the Academy Trust.

Committee Responsible	Staff Student
Lead Member	CEO
Approved by	Policy Review Committee
Date Approved	21 st June 2018
Version	1
Review Date	May 2019



Contents

Introduction	3
Board of Directors	3
Heads of School/Headteachers/Principals and Line Managers	3
Employees	3
Underpinning Principles of this policy	3
Reporting breaches of standards of good conduct	4
1. Whistleblowing	4
2. Confidentiality	5
3. Sharing Information	5
4. Responsibility of employees in possession of sensitive information	7
5. Disclosure of Information	8
7. Personal Use	8
8. Use of email and internet at home	9
9. Security	9
10. Privacy	10
11. Email/IT Protocols	10
12. Data protection	11
13. Social networking	12
14. Relationships	15
15. Neutrality	17
Appendix A - Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings (DCSF 2009)	19
Appendix B - Email Good Practice Guide	19
Appendix C - Examples of unacceptable behaviour using social networking sites	21
Appendix D - Public Interest Disclosure (Whistleblowing) Act 1998	22
Appendix E – Dress Code	24

THE CHELMSFORD LEARNING PARTNERSHIP – CODE OF CONDUCT POLICY

Introduction

The Board of Trustees are committed to providing a professional and ethical environment, which serves and protects the whole education community. Certain expectations for good conduct are described in specific policies and procedures e.g. staff discipline and dismissal, equal opportunities, and professional expectations are set out in national and local conditions of service and in the national 'Teacher Standards'). This policy supplements these provisions and provides additional guidance for adults working in the Academy Trust.

The overriding expectation is that adults will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students public in general and all those with whom they work. This means that adults should not behave through words, actions or inaction in a manner which would lead any reasonable person to question their suitability to work with children or act as a role model. This policy applies to all those working at the Academy Trust including supply staff and voluntary workers. Reference to employees in the policy includes all of these workers. Any breaches of the Code of Conduct Policy will be regarded as a serious matter which could result in disciplinary action, and possible dismissal.

Board of Trustees

It is the responsibility of the Board of Directors to establish and monitor standards of conduct and behaviour, including the establishment of relevant policies and procedures.

Heads of School /Headteachers/Principals and Line Managers

It is the responsibility of the Heads of School/Headteachers/Principals and Line Managers to address promptly any breaches of good conduct and behaviour, using informal procedures where possible but implementing formal procedures where necessary.

Employees

It is the responsibility of all employees to familiarise themselves, and comply, with this policy and all procedures, conditions of service and relevant professional standards.

Underpinning Principles of this policy

- the welfare of the child is paramount
- it is the responsibility of all adults to safeguard and promote the welfare of children and young people. This responsibility extends to a duty of care for those adults employed, commissioned or contracted to work with children and young people
- adults who work with children are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions
- adults should work and be seen to work, in an open and transparent way
- the same professional standards should always be applied regardless of culture, disability, gender, language, racial origin, religious belief and/or sexual identity
- adults should continually monitor and review their practice and ensure they follow the guidance contained in this document

Appendix A sets out guidance on safer working practices which all workers are expected to follow. This guidance is to be read in conjunction with the Academy Trust's Child Protection Policy and

other relevant policies.

Reporting breaches of standards of good conduct

There is an expectation that all employees will provide the highest possible standard of service and care to all those in the Academy Trust community through the performance of their duties. Furthermore, the Board of Trustees is committed to achieving high standards of integrity and accountability and expects the same commitment from its employees and others working in or for the Academy Trust. As such the Board of Trustees wishes to promote an open environment that enables staff to raise issues in a constructive way and with confidence that they will be acted upon appropriately without fear of recrimination.

All employees will be expected to bring to the attention of their Line Manager, any deficiency in the provision of service or care. Employees must report to the appropriate Manager/Board of Directors any impropriety or breach of policy.

Procedures for reporting concerns are set out at Appendix D.

1. Whistleblowing

This section should be read in conjunction with the Academy Trust's Whistleblowing Policy.

Where an employee considers that internal measures have not been taken in respect of any concerns they have raised, they may make a Public Interest Disclosure (commonly known as Whistleblowing). The Act affords protection against dismissal or penalty where an employee discloses certain information relating to:

- failure to comply with legal obligation
- miscarriages of justice
- criminal offences
- danger to Health and Safety
- damage to the environment, and
- concealment of evidence relating to the above

To qualify for protection the employee must have acted in good faith and have reasonable grounds for belief in the disclosure. The employee should usually have raised the matter internally prior to making a Public Interest Disclosure. Disclosures are only protected if made to the employer/some other person responsible for the matter/regulatory body.

This procedure should be used where the concern is about the consequences for other employees or the public. If the concern is about employees being disadvantaged by the action or failure to take action of others, then that should be pursued through the Academy Trust's grievance procedure.

It is important that where deficiencies in service provision standards are involved rather than corruption, staff should satisfy themselves that the failing is serious and that the potential disadvantage to the public or the Academy Trust is significant. Any unnecessarily over-zealous reporting would be inappropriate and counter-productive.

In all cases employees may wish to seek advice from their professional association/trade union

before making a protected disclosure.

Further details on the Whistleblowing procedure can be found in Appendix D.

2. Confidentiality

Working in the Academy Trust environment means having access, in a variety of ways, to information that must be regarded as confidential. As a general rule, all information received in the course of employment, no matter how it is received, should be regarded as sensitive and confidential.

Employees should use their discretion regarding these matters, and should seek further advice from their Line Manager.

All workers and volunteers must be aware that they may be obliged to disclose information relating to child protection issues and should make it clear to the individual either that confidentiality cannot be guaranteed and/or decline to receive the information and direct them to a more appropriate colleague.

Employees should have regard to potential difficulties which may arise as a result of discussions outside work. While it is natural to talk about work at home or socially, employees should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on. Employees should be particularly aware that many people will have a direct interest in the Academy Trust and even the closest of friends may inadvertently use information gleaned through casual discussion. In particular, employees need to understand the implications of discussions on social media sites (see section 8).

Information that is regarded as confidential can relate to a variety of people e.g. pupils, parents, staff, Trustees or job applicants and a variety of matters for example personal information, conduct and performance, health, pay, internal minutes etc.

Confidential information can take various forms and be held and transmitted in a variety of ways e.g. manual records (files, reports, and notes), computerised records, telephone calls, face-to-face and email.

The methods of acquiring information can also vary. Individuals and groups may become aware of confidential information in the following ways:

- access is gained as part of the employees day to day work
- information is supplied openly by an external third party
- employees may inadvertently become aware of information

3. Sharing Information

While it is often necessary to share such information, in doing so, employees should consider the following key points:

- how sensitive is the information?
- how did it come to your attention?
- who does the information need to be shared with?
- for what purpose?
- who is the information being copied to? and why?

- does restriction of access need to be passed on to your audience?
- the most appropriate method of communication e.g. verbal, written, email, in person
- the potential consequences of inappropriate communication
- it is also an individual employee's responsibility to safeguard sensitive information in their possession

Within the course of daily operation, information related to the Academy Trust or those connected with it, may be requested by, supplied by, or passed to a range of people. This might include internal colleagues, pupils, Trustees, trade unions, parents, the local authority, Department for Education and contractors.

Clearly, the sensitivity of the information will be partly dependent upon the recipient /supplier and the manner in which it is transferred.

Particular responsibilities are:

- personal (e.g. home addresses and telephone numbers) and work-related information (e.g. salary details, medical details) relating to individuals, should not be disclosed to third parties except where the individual has given their express permission (e.g. where they are key holders) or where this is necessary to the particular work being undertaken, eg. it is necessary for an individual to be written to
- if someone requesting information is not known to staff, particularly in the case of telephone calls, his/her identity and the legitimacy of his/her request should be verified by calling them back. A person with genuine reasons for seeking information will never mind this safety measure. It is a requirement under the Data Protection Act 1998 that action is taken to ensure the validity of any caller even if they state they have a statutory right to the information requested
- wherever possible requests for information should be made in writing e.g. employee references
- the same principle applies when sending emails. Staff should always check that the information is going to the correct person and is marked confidential where appropriate
- being known as an employee of the Academy Trust may mean being asked for information, for instance, by parents about a member of staff who is off sick. Although this can be awkward, parents must be informed that employees are unable to discuss confidential matters. Persistent enquiries should be referred to their Line Manager
- the Data Protection Act 1998 refers to the principle of third party confidentiality. Information relating to, or provided by, a third party should not be released without the written consent of the third party or unless an "order for disclosure" is made by a court of competent jurisdiction

A variety of phrases may be used on correspondence to denote confidentiality. As a general rule:

- post marked "personal" or "for the attention of the addressee only" should only be opened by the addressee personally

- post marked “private and/or confidential” may be opened by those responsible for distributing post within the Academy Trust

Confidential mail which is then forwarded internally should continue to carry a confidential tag.

4. Responsibility of employees in possession of sensitive information

Employees have a responsibility to make sure sensitive information is stored securely.

They should:

- make sure filing cabinets are kept locked when unattended
- make sure sensitive information is not left on desks or the photocopier/fax/printer
- make sure papers are not left lying around at home or in the car. If confidential materials or paperwork are taken out of the office, precautions must be taken to ensure they are not accessible to third parties
- make sure appropriate steps are taken to keep track of files which are on loan or being worked on i.e. a record of the date sent and the recipient’s name and position;
- make sure, if it is necessary to supply personal files through the external mail, these are sent recorded delivery
- make sure copies of emails are stored securely
- make sure steps are taken to ensure that private/confidential telephone calls/conversations are not overheard
- make sure meetings where sensitive or confidential information is being discussed are held in a secure environment
- make sure confidential paperwork should be disposed of correctly either by shredding it or using the confidential waste facility
- make sure personal data is not used for training or demonstration purposes where fictional data can be used
- make sure Line Managers comply with the procedures for the storage and sharing of information relating to individuals performance management reviews

Employees also have a responsibility to make sure computer data is stored securely.

They should:

- make sure computer data is not left exposed to others view when unattended – screen savers/screen lock should be used
- make sure machines are switched off/you are logged off when leaving the office or classroom
- passwords should not be disclosed to other colleagues unless absolutely necessary
- make sure sensitive data should not be stored on public folders
- staff should be familiar with the security of email/internet systems
- make sure any user IDs and passwords remain confidential;

5. Disclosure of Information

Both during and on leaving the employment of the Board of Trustees, employees must not divulge information of a confidential, sensitive or commercial nature gained during the course of employment for purposes detrimental to the interests of the Board of Trustees, its employees or clients. In the case of any commercially sensitive information the condition applies for a period of 12 months after leaving employment.

If during the course or as a result of employment an employee invents or designs anything which has some connection with the work, details of the invention or design must not be disclosed to anybody until the matter has been reported to the Heads of School/Headteachers/Principals and permission has been given. The right to register the design or patent the invention may be lost by a premature disclosure of its nature and as a result personal interest or that of the Board of Directors might be prejudiced.

6. Use of computers, email and the internet

This section should be read in conjunction with the Academy Trust's Social Media Policy.

The email system and the internet are extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. The use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications is encouraged.

Those using the Academy Trust's electronic mail services and/or the internet are expected to do so responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

Computers and laptops loaned to employees by the Academy Trust are provided to support their professional responsibilities and employees must not use their employer's equipment for any significant personal use. Reasonable access and use of the internet and email facilities is also available to recognised representatives of professional associations' i.e. union officers.

Employees must not use Academy Trust equipment or property for personal gain or fraudulent, malicious, illegal, libelous, immoral, dangerous, offensive purposes.

Employees should not undertake IT related activities that are contrary to the Academy Trust's policies or business interests including accessing, downloading, storing, creating, copying or distributing offensive material (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

All forms of chain mail are unacceptable and the transmission of user names, passwords or other information related to the security of the Academy Trust's computers is not permitted.

7. Personal Use

The Academy Trust's e-mail and internet service may be used for incidental personal purposes, with the approval of the line manager, provided that it does not:

- interfere with the Academy Trust's operation of computing facilities or email services
- interfere with the user's employment or other obligations to the Academy Trust
- interfere with the performance of professional duties
- is of a reasonable duration and frequency
- is performed in non-work time
- does not over burden the system or create any additional expense to the Academy Trust
- does not bring the Academy Trust and its employees into disrepute

Such use must not be for:

- unlawful activities;
- commercial purposes not under the auspices of the Academy Trust;
- personal financial gain;
- personal use that is inconsistent of other Academy Trust policies or guidelines.

If an employee fails to meet these conditions for personal use, their rights to use equipment may be withdrawn. If an employee fails to follow this policy and other supporting procedures, this could result in disciplinary action.

8. Use of email and internet at home

Access to the internet from an employee's home using an Academy Trust owned computer or through Academy Trust owned connections must adhere to all the policies that apply to their use.

Family members or other non-employees must not be allowed to access the Academy Trusts computer system or use the Academy Trust's computer facilities, without the formal agreement of their line manager.

9. Security

The Academy Trust follows sound professional practices to secure email records, data and system programmes under its control. As with standard paper based mail systems, confidentiality of email cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered emails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

In order to effectively manage the email system, the following should be adhered to:

- open mailboxes must not be left unattended
- care should be taken about the content of an email as it has the same standing as a memo or letter. Both the individual who sent the message and/or the Academy Trust can be sued for libel
- reporting immediately to IT units when a virus is suspected in an email

10. Privacy

The Academy Trust respects user's privacy. Email content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- when required by law
- if there is a substantiated reason to believe that a breach of the law or Academy Trusts policy has taken place
- when there are emergency or compelling circumstances

The Academy Trust reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies. Employees will be notified of any monitoring which will take place and the reason for it. Monitoring will be reasonable and in accordance with Data Protection and Human Rights obligations.

Employees should not have any expectation of privacy to his or her internet usage. The Academy Trust reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy.

Auditors must be given the right of access to any document, information or explanation that they require.

Use of the employees designated personal file area on the network server provides some level of privacy in that it is not readily accessible by other members of staff. These file areas will however be monitored to ensure adherence to policies and to the law.

Managers will not routinely have access to an employee's personal file area. However, management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

11. Email/IT Protocols

A good practice guide for employees on the use of emails is available at Appendix B.

Users must:

- respond to emails in a timely and appropriate fashion. The system is designed for speedy communication. If urgent, the email requires a prompt response, otherwise a response should be sent within a reasonable timeframe according to the nature of the enquiry. This should be, wherever possible, within 2 working days
- not use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any internet service which requests name, e-mail address or other details
- not abuse others, even in response to abuse directed at themselves
- not use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access

and use the system

- not use, transfer and tampering with other people's accounts and files
- not use their own equipment to connect to the Academy Trusts network unless specifically permitted to do so and the equipment meets appropriate security and other standards. Under no circumstances is personal equipment containing inappropriate images or links to them, to be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children
- adults should ensure that pupils are not exposed to any inappropriate images or web links. Academy Trust service and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential
- not store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices
- memory sticks (all disks/memory sticks used must be encrypted and/or password protected)
- respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner
- not use the internet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations

If a user finds him/herself connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to their line manager. Any failure to report such access may result in disciplinary action.

Except in cases in which explicit authorisation has been granted by an appropriate manager, employees are prohibited from engaging in, or attempting to engage in:

- monitoring or intercepting the files or electronic communications of other employees or third parties
- hacking or obtaining access to systems or accounts they are not authorised to use
- using other people's log-ins or passwords
- breaching, testing, or monitoring computer or network security measures
- interfering with other people's work or computing facilities
- sending mass e-mails without consultation with the Head teacher. Global sends (send to everybody in the Global address book) are prohibited

12. Data protection

The Data Protection Act 1998 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to e-mail in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, the Academy Trust respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As data controller, the Academy Trust has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998.

In order to comply with its duties under the Human Rights Act 1998, the Academy Trust is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account the Academy Trust's wider business interests. In drawing up and operating this policy the Academy Trust recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of the Academy Trust's IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance.

13. Social networking

This section should be read in conjunction with the Academy Trust's Social Networking Policy.

The purpose of this policy is to ensure:

- that Academy Trust is not exposed to legal and governance risks
- that the reputation of the Academy Trust is not adversely affected
- that our users are able to clearly distinguish where information has been provided via social networking applications, that it is legitimately representative of the Academy Trust
- protocols to be applied where employees are contributing in an official capacity to social networking applications provided by external organisations

Social networking applications include but are not limited to:

- blogs i.e. blogger
- online discussion forums, for example Facebook, Twitter etc
- media sharing services for example YouTube/Facebook
- micro-blogging applications, for example Twitter

Academy Trusts managing social networking sites

It is important to ensure that employees, members of the public and other users of online services know when a social networking application is being used for official Academy Trust purposes. To assist with this, all employees must adhere to the following requirements:

- only use an official (ie not personal) email addresses for user accounts which will be used for official purposes
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users

- the Academy Trusts logo and other branding elements should be used where appropriate to indicate the Academy Trusts support. The Academy Trusts logo should not be used on social networking applications which are unrelated to or are not representative of the Academy Trusts official position
- employees should identify themselves as their official position held within the Academy Trust on social networking applications. eg through providing additional information on user profiles
- employees should ensure that any contributions on any social networking application they make are professional and uphold the reputation of the Academy Trust – the general rules on internet/email apply
- staff should not spend an unreasonable or disproportionate amount of time during the working day developing, maintaining or using sites
- employees must not promote or comment on personal, political, religious or other matters
- employees should be aware that sites will be monitored

Personal social networking sites

All employees of the Academy Trust should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation and the Safeguarding Vulnerable Groups Act 2006. Employees must also operate in line with the Academy Trusts Equality and Diversity policy.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the Academy Trust community.

Employees hold positions of responsibility and are viewed as such in the public domain. Inappropriate usage of social networking sites by employees can have a major impact on the employment relationship. Any posting that causes damage to the Academy Trust, any of its employees or any third party's reputation may amount to misconduct or gross misconduct which could result in dismissal.

Employees should not use personal site for any professional activity. The Academy Trust reserves the right to require the closure of any applications or removal of content published by employees which may adversely affect the reputation of the Academy Trust or put it at risk of legal action.

Anyone who becomes aware of inappropriate postings on social networking sites, must report it to their line manager as soon as possible. The line manager will then follow the disciplinary procedure. If an employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate and falls within the remit of this policy, then that employee may be subject to the disciplinary procedure.

Posting inappropriate images

Indecent images of any employee that can be accessed by students, parents or members of the public are totally unacceptable and can lead to child protection issues as well as bringing the Academy Trust into disrepute.

Posting inappropriate comments

It is totally unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the Academy Trust community on any type of social networking site.

Reports about oneself may also impact on the employment relationship for example if an employee is off sick but makes comments on a site to the contrary.

Social interaction with pupils (past and present)

Employees should not engage in conversation with pupils, past or present, irrespective of their age, on any social networking site. Offers of assistance to a pupil with their studies via any social networking site are inappropriate and also leaves the employee vulnerable to allegations being made. It would be very rare for employees to need to interact with pupils outside of Academy Trust in a social setting and by communicating with them on social networking sites, is tantamount to the same.

Adults should ensure that personal social networking sites are set at private and that pupils are never listed as approved contacts. Adults should not use or access social networking sites of pupils.

Should an employee become aware of an underage person using social networking sites, then they should report this to the site operator and if that child is at their particular Academy Trust, then this should be reported to their line manager.

Making Friends

Employees should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. Again this may leave employees vulnerable to allegations being made.

General Terms of use

All employees must adhere to the following terms of use of social networking applications. This includes, but is not limited to public facing applications such as open discussion forums and internally-facing applications, (ie. e-folio) regardless of whether they are hosted on organisational networks or not.

The Academy Trust expects that users of social networking applications will always exercise due consideration for the rights of others and strictly in accordance with the following terms of use.

Social networking applications must not:

- be used to publish any content which may result in actions for breach of contract, defamation, discrimination, breaches of copyright, data protection, breach of confidentiality, intellectual property rights or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the Academy Trust or the local authority into disrepute. Some examples are given in Appendix C
- be used for party political purposes of specific campaigning purposes as the local authority is not permitted to publish any material which „in whole or part appears to

- affect public support for a political party" (LGA 1986)
- be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- be used in an abusive or hateful manner
- be used for actions that would put other employees in breach of the Code of Conduct Policy
- be in breach of the Academy Trusts disciplinary and equal opportunities policies

Where individuals from partner organisations are involved and are acting on behalf of the Academy Trust, they will also be expected to comply with the relevant policies.

14. Relationships

Board of Trustees proceedings

There are restrictions on Trustees or persons taking part in proceedings of the Board of Trustees or their committees under the Education (Government) (England) Regulations 1999 which requires that they shall withdraw:

- if there is a conflict of interest or where there is reasonable doubt about their ability to act impartially
- where they have pecuniary interest, for example contracts
- if a relative (including spouse) living with them has pecuniary interest

The community and service users

Employees must always remember their responsibilities in the community they serve and ensure courteous, efficient and impartial service delivery to all groups and individuals within the community as defined by the policies of the Board of Directors and, where applicable, the local authority.

Contracts

All relationships of a business or private nature with external contractors, or potential contractors, must be made known to Board of Directors. Orders and contracts must be in accordance with standing orders and financial regulations of the county council and the Academy Trust. No special favour should be shown to businesses run by, for example, friends, partners or relatives in the tendering process.

Employees who engage or supervise contractors or have any other official relationship with contractors and have previously had or currently have a relationship in a private or domestic capacity with contractors, must declare that relationship to the Academy Trusts Board of Directors.

Gifts, Legacies, Bequests and Hospitality

Employees may not accept any gift or legacy from a person intended to benefit from their services (or those whom they supervise) or from any relative of theirs without the prior written permission the Heads of School/Headteachers/Principals. Employees may not give any gift to someone from whom they expect to receive any favour in their official capacity. Employees must declare all gifts with a value of over £50, even if these come from

parents/families as a 'thank you'.

Hospitality offered to an employee's official capacity should only be accepted if that is part of a genuine business activity. Any such hospitality should be properly authorised and recorded by the Heads of School/Headteachers/Principals

Employees should always consider any particular sensitivities around accepting hospitality from an organisation that may be affected by decisions being taken by the Board of trustees.

Whilst employees may accept gifts of token value such as pens and diaries, they should not accept personal gifts from contractors or outside suppliers.

Failure to observe these rules will be regarded as gross misconduct: See Appendix A for gifts in respect of pupils.

Close personal relationships at work

Situations arise where relations, or those in other close relationships, may be employed at the Academy Trust and it is recognised that close personal relationships can be formed at work.

Close personal relationships are defined as:

- employees who are married, dating or in a partnership or co-habiting arrangement
- immediate family members for example parent, child, sibling, grandparent/child
- other relationships for example extended family (cousins, uncles, in-laws), close friendships, business associates (outside the Academy Trust). Whilst not all such situations where those in close personal relationships work together raise issues of conflict of interest, implications can include
- effect on trust and confidence
- perception of service users, the public and other employees on professionalism and fairness
- operational issues e.g. working patterns, financial and procurement separation requirements
- conflicting loyalties and breaches of confidentiality and trust

Open, constructive and confidential discussion between employees and managers is essential to ensure these implications do not occur.

Management

It is inappropriate for an employee to line manage or sit on an appointment panel, for those with who they have a close personal relationship. Employees must not be involved in any decisions relating to discipline, promotion or pay adjustment for anyone where there is a close personal relationship. If this was the case, the Heads of School/Headteachers/Principals would need to identify another individual to undertake the particular responsibility, so that a "conflict of interest" situation is avoided.

Any applicants applying for positions are required to disclose on their application form if they:

- are a relative or partner of, or
- have a close personal relationship with any employee in the Academy Trust

Applicants are asked to state the name of the person and the relationship. Failure to disclose such a relationship may disqualify the applicant.

Employees should discuss confidentiality with their Head teacher/line manager, any relationships with an applicant.

If a close personal relationship is formed between two colleagues who are working in the Academy Trust this should be disclosed, in confidence, to the line manager by the employees concerned as this may impact on the conduct of the Academy Trust.

It is important to ensure that any approach or actions are not unfair or discriminatory. Nevertheless it is important to explore, in discussion with the employees concerned, the issues that may arise to ensure these can be managed effectively.

Impact

It may be appropriate to employ someone to work in a team with someone with who they have a close personal relationship. It may also be necessary in certain circumstances to consider transferring staff that form close personal relationships at work. Any such action will be taken wherever possible by agreement with both parties and without discrimination.

Colleagues who feel they are affected by a close personal relationship at work involving other colleagues should at all times feel that they can discuss this, without prejudice, with their Head teacher/line manager, other manager or Board of Directors.

References

When providing a reference, the individual providing the reference must make it clear if it is provided as a personal or colleague reference or provided formally as a reference on behalf of the employer.

Personal or colleague references should not be provided on headed paper. References on behalf of the employer should be cleared and signed by another manager.

15. Neutrality

Employees serve the community as a whole. It follows they must serve all members of the Academy Trust community and the public and ensure that the individual rights of all of these groups are respected. Employees must not allow their own personal, political, religious or other views and opinions to interfere with their work.

Political Restriction

Certain local government employees are restricted from political activity and where such restrictions exist, these are outlined in employee's contract of employment.

Use of financial resources

Employees must ensure that they use public and any other funds entrusted to them in a responsible and lawful manner. They must strive to ensure value for money to the local

community and to avoid legal challenge to the Board of Directors or the local authority. They must also observe the county councils financial regulations and Academy Trust's financial regulations.

Sponsorship

Where an outside organisation wishes to sponsor or is seeking to sponsor an Academy Trust activity, whether by invitation, tender, negotiation or voluntarily, the basic conventions concerning acceptance of gifts or hospitality apply. The sponsorship should always be related to the Academy Trust's interests and/or the authority's departmental or corporate activities and never for personal benefit only. Particular care must be taken when dealing with contractors or potential contractors.

Appendix A - Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings (DfE 2015)

Below are the key expectations set out in the Guidance. A copy of the full document can be accessed : <H:\Downloads\Guidance-for-Safer-Working-Practices-2015-final1.pdf>

Appendix B - Email Good Practice Guide

Good Practice	
Read receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the „read receipt“ option.
Attachment formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
E-mail address groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of e-mails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one person use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own e-mail address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the „out of office“ message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of e-mails could be used in support, or in defence, of the Academy Trusts legal position in the event of a dispute.

Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the e-mail can result in legally binding contracts being put into place.
Distribution lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them
E-Mail threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	E-mail in the right context, care should be taken to use e-mail where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as shouting so consider how the style of your email may be interpreted by its recipient.
Forwarding e-mails	Consideration should be given when forwarding e-mails that it may contain information that you should consult with the originator before passing to someone else.
Large e-mails	For larger e-mails, particularly Internet e-mails, where possible send at the end of the day as they may cause queues to form and slow other people's e-mail.

Appendix C - Examples of unacceptable behaviour using social networking sites

1. Breach of contract

There is an implied term of mutual trust and confidence between employer and employee in all employment contracts. A very negative and damaging posting or communication on a social networking site about the Academy Trust or colleagues may entitle the Head teacher/line manager to decide that this term has been broken. Such conduct would be subject to the Academy Trusts disciplinary procedure and could warrant the employee's dismissal.

Emails are capable of forming contractual documents. Contracts can easily be formed by careless emails and non-compliance with the terms of any such contracts will render an organisation liable for a breach of contract claim. Emails tend not to be subject to the same safeguard procedures as paper documents which are often checked before they are signed off.

2. Defamation

If an employee places defamatory information or material on a social networking site such as bad mouthing another colleague or a pupil of the Academy Trust, such conduct would be subject to the Academy Trusts disciplinary procedure and could lead to the employee's dismissal.

3. Discrimination

The Academy Trusts recruitment and selection policy provides the correct and proper procedures to be used in the recruitment and selection of staff. Candidates should be selected on the basis of testable evidence provided on application forms and through the selection process and references as provided by the applicant. Under no circumstances should information from social networking sites be used to make selection decisions. Such action could result in expensive discrimination claims. For example - not all candidates will have profiles on social networking sites and using information from this source may be seen as giving an unfair advantage or disadvantage to certain candidates, possibly discriminating against younger people who are likely to use social networking sites more often.

Many forms of discrimination claims, including harassment claim can occur via emails, If an employee places discriminatory material about another employee, a member of the Board of Directors, parents, children, young people, and vulnerable adults, this could amount to bullying or harassment of that individual. The Academy Trust may be vicariously liable for such acts unless it took such steps that were reasonably practicable to prevent material being placed on a site. Where an employee carries out an act of harassment or discrimination in the course of their employment, the Academy Trust is vicariously liable for that act even when the act is unauthorised. Once an issue of email harassment has been raised and the harasser identified, immediate action should be taken to stop the harassment and instigate the disciplinary procedure while supporting the harassed employee.

4. Breach of health and safety

For example an internet video clip of employees performing stunts wearing the organisations uniform. When information like this is found, the Academy Trust should follow the company's disciplinary procedure to investigate the possibility of a breach of health and safety legislation on the part of the employee. If an Academy Trust is aware of this and fails to investigate there may be liability for personal injuries in the law of negligence.

Appendix D - Public Interest Disclosure (Whistleblowing) Act 1998

1. Raising Concerns

Staff should raise any concerns about the conduct or behaviour of employees, volunteers or others associated with the operation and organisation of the Academy Trust as soon as possible. Verbal reports should be followed up in writing.

Concerns should normally be raised initially with the employee's line manager. However, where the complaint relates to the employee's line manager, the complaint should be brought to the attention of a more senior manager, the Head teacher/Principal or the Chair of Directors.

2. Whistleblowing

Where having raised a concern there is a genuine belief that the Academy Trust has failed to take appropriate action, a report should be made to the Chair of Directors or in exceptional circumstances the Local Authority.

Where the complaint is serious for example involving fraud, theft or other potential gross misconduct, act quickly to report it but do not mention it to the subject of the complaint or other colleagues as that could prejudice any investigatory process.

It may be the case that you will have very genuine and justified suspicions of wrong-doing even though at the time of reporting you cannot point to concrete evidence. That should not deter you from going ahead and reporting the matter, particularly where it may involve potential risk to vulnerable people.

3. Action by recipients of disclosures

It would be inappropriate to have hard or fast rules and judgement must be exercised. While it is essential for problems to be tackled effectively and with the aim of righting wrongs, this may well be best achieved in many less serious cases by discussion with the „offending“ employee and securing a commitment as to future standards and corrective action. In other more serious cases the matter may need to be passed to a more senior level of management or directly to the Board of Directors, as appropriate.

Where complaints are received from members of the public, the Academy Trusts formal complaints procedure (as contained in the Academy Trust Customer Care Code of Practice) must be followed, unless the complaint relates to the specific conduct or performance of an individual employee in which case the Disciplinary Procedures may need to be instigated.

Any written complaint/allegation should be given a written acknowledgement and confirmation that the matter will be looked into. Unless clearly made in a very low key way about minor matters, verbal complaints/allegations should receive a written acknowledgement in the same way

In the event of the allegation being of a very serious nature, for example relating to a fraud or other potential gross misconduct offence, there may well be a need to involve the Academy Trusts auditors and/or the police. This should normally be agreed initially by the Chair of Directors who should, in turn, and where appropriate, keep the Local Authority informed in view of any possible implications concerning public monies. Advice may be sought from the Academy Trusts legal advisors before involving the police in any such internal complaint or allegation.

When any complaint or allegation has been looked into and resolved or dealt with, the person who raised the matter in the first instance should be notified of that, normally in writing unless common-sense indicates that it can be done more appropriately in a verbal, informal way. How much detail to give of findings and outcomes is a matter of judgement and it would, for example, be inappropriate to disclose details of disciplinary actions taken against another employee.

4. Protecting ‘whistleblowers’ and complainants

A ‘whistleblower’ may ask for their identity to be kept concealed. Frequently the answer will be yes, but in more serious cases where disciplinary action may have to be taken against others they may well have a right to know the source as well as the nature of such complaints. In any case the Academy Trust is committed to doing as much as possible to ensure that well-being at work does not suffer as a result of the tensions that may result from the making or investigation of complaints.

If a person believes they are experiencing harassment or victimisation at work as a consequence of ‘whistleblowing’ they are strongly encouraged to bring this to an appropriate senior manager’s attention at an early stage so that it can be addressed. The Academy Trust will take any appropriate action necessary to ensure that such harassment or victimisation stops.

Whether or not work relationships suffer in this way it may well be that ‘whistleblowers’ will find the process of reporting wrong-doing and making statements etc. stressful, particularly where there may be feelings of divided loyalties. In such circumstances the “whistleblower” may welcome the opportunity to talk through these anxieties and feelings either with their manager or possibly, with someone from a counselling service. This is to be encouraged.

5. What if I receive a complaint about myself?

If the complaint or allegation is at all significant or made in a formal way, particularly by a member of the public or other external users, then you should inform your line manager or Chair of Directors in the case of Head teachers – even if you believe or know the complaint to be groundless or unjustified.

Where a complaint or grumble clearly does not justify taking up the line in this way, making a brief note on a file or diary or similar will often be appropriate and in your own best interests.

6. Malicious accusations

If, on investigation, it is considered that an employee has made malicious allegations without real substance, then that in itself will be taken as a most serious matter and likely to result in disciplinary action.

Appendix E – Dress Code

It is felt appropriate to raise with staff the need for professionalism in their attire for work. This will assist in the drive to improve student uniform. This issue has been raised by members of staff following negative comments made by external visitors and, also, when staff have felt uncomfortable with staff dress.

We would hope that staff will self-regulate on dress but to help in this decision-making a list as to what should not be worn is detailed below. Please note that this list is indicative, not exhaustive.

- Jeans or jean-style trousers
- Denim
- Trousers which are worn so low on the hips as to expose underwear
- Shorts
- Leggings
- See-through tops
- Vest-style tops
- Strapless tops or dresses
- Tops which are so tight as to expose stomachs or backs
- Tops or dresses with shoestring straps unless they are covered by a jacket or cardigan
- Very short skirts
- $\frac{3}{4}$ length trousers unless they are smart, suit style material
- Flip flops/backless sandals – this is particularly important with respect to health and safety in corridors and on stairs

Although it is acceptable for men not to wear a tie if the rule has been relaxed for students during the summer, at all other times ties should be worn correctly with the top button of the shirt done up.

It is recognised that there may be some variations as a result of the area in which you work, for example PE.