The Thrive Partnership Academy Trust

Code of Conduct Policy

Document Detail	
Authorised By:	Board of Directors
Version:	1
Status:	Approved on 25 January 2017
Next Scheduled Review Date:	January 2018

Changes November 2014

Item No.	Heading	Details of Change details
4	Safer Working Practices	Reference and link to updated non-statutory guidance
Appendix A	Safer Working Practices	Removed. Replaced by references and link in Section 4 to full guide. Subsequent Appendices renumbered

Changes September 2015

Item No.	Heading
Appendix D	Whistleblowing Policy
2.1	Scope
3.3	Roles and responsibilities
7	Use of computers, email and the internet
8.3.5	Personal social networking sites (political and financial purposes)
11	Gifts, legacies, bequests and hospitality

Contents Page

1. Introduction

1.1 The Trust Board is 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. Disciplinary Procedure, Equality and Diversity in Employment Policy, Recruitment Policy and professional expectations are set out in national and local conditions of service and by relevant professional bodies. This policy supplements these provisions and provides additional guidance for employees and individuals engaged to work in the Trust.

1.2 The overriding expectation is that employees and those engaged to work in the Trust will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, the public in general and all those with whom they work or come into contact with in the course of their employment or engagement by the Trust.

This means that employees and those engaged to work in the Trust 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.

2. Scope

2.1 This Code applies to all individuals employed or engaged by the Trust including:

- relief/supply staff
- voluntary workers

All provisions of this Code are applicable to employees. Employees will be provided with a copy of this Code, will be consulted on any changes and will be provided with any amendments. Employees must familiarise themselves with the content of this Code and any updates as soon as they are available.

For engaged workers and volunteers, this code applies in so far as specific provisions are relevant to the role they are performing within the Trust. These workers and volunteers should familiarise themselves with the relevant provisions of this Code at the earliest opportunity.

2.2 Any breaches of this Code of Conduct Policy will be regarded as a serious matter which could result in disciplinary action, and in certain circumstances could potentially lead to dismissal.

3. Roles and responsibilities

3.1 Trust Board

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

3.2 Chief Executive Officer/Executive Principal/Head of Trust and Line Managers

It is the responsibility of Chief Executive Officer/Executive Principal/Head of Trust and Line Managers to address promptly any breaches of good conduct and behaviour, using informal procedures where possible but implementing formal procedures where necessary.

3.3 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.

It is an express term of each employee's employment with the Trust that any wrongdoing or alleged wrongdoing by the employee (regardless of whether the employee denies the wrongdoing/alleged wrongdoing), including any incidents arising from alternative employment or outside of work which may have a bearing on the employee's employment with the Trust, must be disclosed to the Trust immediately. Any such disclosure should be to the Chief Executive Officer/Executive Principal/Head of Trust, in the case of the Chief Executive Officer to the Trust Board and in the case of the Executive Principal/Head of Trust to the Chief Executive Officer. Failure to disclose any wrongdoing or alleged wrongdoing will be considered a serious matter which could result in disciplinary action, and in certain circumstances could potentially lead to dismissal. Any such disclosure (and any action arising from it (if any)) will be considered in the context of the individual circumstances and taking into account all the relevant factors including (but not limited to) the seriousness/level of the disclosed information and the individual's role within the Trust.

4. Safer Working Practice with Children and Young People

It is important that all adults working with children understand that the nature of their work and the responsibilities related to it, place them in a position of trust. Adults must be clear about appropriate and safe behaviours for working with children in paid or unpaid capacities, in all settings and in all contexts.

The relevant requirements are set out in the Trust's Child Protection and Behaviour

Management Policies and Procedures and in the **DfE Statutory Guidance "Keeping Children Safe in Education" (March 2015, as amended). This is the key statutory guidance which all employees must follow and all employees and volunteers must, as a minimum, read Part 1 of that Document.**

Below is a broad overview of the key expectations for adult's interactions with children and young people as set out in "Guidance for Safer Working Practice for those working with Children and Young People in Education Settings"
http://www.saferrecruitmentconsortium.org/GSWP%20Oct%202015.pdf

These documents should be read in conjunction with the body of the Code of Conduct and other relevant Trusts policies and procedures.

4.1 Underpinning Principles

- The welfare of the child is paramount
- Staff should understand their responsibilities to safeguard and promote the welfare of pupils
- Staff 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
- Staff should work, and be seen to work, in an open and transparent way
- Staff should acknowledge that deliberately invented/malicious allegations are extremely rare and that all concerns should be reported and recorded
- Staff should discuss and/or take advice promptly from their line manager if they have acted in a way which may give rise to concern
- Staff should apply the same professional standards regardless of culture, disability, gender, language, racial origin, religious belief and sexual orientation
- Staff should not consume or be under the influence of alcohol or any substance, including prescribed medication, which may affect their ability to care for children
- Staff should be aware that breaches of the law and other professional guidelines could result in disciplinary action being taken against them, criminal action and/or other proceedings including barring by the Disclosure & Barring Service (DBS) from working in regulated activity, or for acts of serious misconduct prohibition from teaching by the National College of Teaching & Leadership (NCTL).
- Staff and managers should continually monitor and review practice to ensure this guidance is followed

- Staff should be aware of and understand their establishment's child protection policy, arrangements for managing allegations against staff, staff behaviour policy, whistle blowing procedure and their Local Safeguarding Children Board LSCB procedures.

5. 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 Trust community through the performance of their duties. Furthermore, the Trust Board 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 Trust. As such the Trust Board 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 an appropriate manager / Trust Board any impropriety or breach of policy. In the event that the concern is not resolved by the employee's line manager or by another appropriate manager, employees may follow the procedure set out in the Whistleblowing policy set out at Appendix C.

5.1 Whistleblowing

5.1.1 Whistleblowing ("protected disclosure") occurs when an employee or worker provides certain types of information, usually to the employer or a prescribed body, which has come to their attention through work. The disclosure may be about the alleged wrongful conduct of the employer, or about the conduct of a fellow employee, or any third party.

Whistleblowing is therefore 'making a disclosure in the public interest' and occurs when a worker raises a concern about danger or illegality that affects others, for example pupils in the Trust or members of the public.

Employees and workers who make a 'protected disclosure' are protected from being subjected to a detriment or being dismissed as a result of making the disclosure. The key piece of legislation is the Public Interest Disclosure Act 1998 (PIDA) ("the Act") which applies to almost all workers and employees, including agency workers and self-employed workers. The provisions of the Act have been supplemented by the Enterprise and Regulatory Reform Act 2013.

The Act affords protection against dismissal or detriment where an employee discloses information relating to:

- a breach of any legal obligation;

- a miscarriage of justice;
- a criminal offence;
- a danger to the Health and Safety of any individual;
- damage to the environment; and,
- deliberate concealment of information about any of the above.

5.1.2 To qualify for protection the employee must believe that they are telling the appropriate person and they must have reasonable grounds for belief in the disclosure. The employee must also reasonably believe that making the disclosure is in the public interest. The employee should usually have raised the matter internally prior to making a protected disclosure. Disclosures are only protected if made to the employer/some other person responsible for the matter/regulatory body. There is a list of prescribed bodies to whom disclosures can be made, depending on the nature of the disclosure.

5.1.3 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 Trust grievance procedure.

5.1.4 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 C.

6. Confidentiality

Working in the 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 or whilst being engaged by the Trust, 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 or the Chief Executive Officer/Executive Principal/Head of Trust, as appropriate.

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.

6.1. Discussions outside work

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 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 networking sites (see section 8).

6.2. Types of confidential information

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

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

6.2.3 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 employee's day to day work;
- information is supplied openly by an external third party;
- employees may inadvertently become aware of information;

6.3. Sharing Information

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

- The nature of the information:
    - how sensitive is the information?;
    - how did it come to your attention?;

- The appropriate audience:
    - 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.

6.3.1 Within the course of daily operation, information related to the 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, governors, trade unions, parents, the local authority, Dept. of Education and contractors.

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

6.3.3 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, e.g. it is necessary for an individual to be written to;
- If someone requesting information is not known to the Trust, 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 a genuine reason 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
- The same principle applies when sending emails and faxes. Employees 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 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 the 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.

6.3.4 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 Trust.

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

6.4. Responsibility of employees in possession of sensitive information

6.4.1 Employees have a responsibility to make sure sensitive information is used and 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 away from the Trust, 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 faxes and 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 is disposed of correctly either by shredding 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.

6.4.2 Employees have a responsibility to make sure computer data is used and stored securely.

They should:

- make sure computer data is not left exposed to others' view when unattended, or when using computers for sensitive data where other employees may have sight of such data – screen savers should be used where appropriate ;
- make sure machines are switched off when leaving the office;
- passwords must not be disclosed to other colleagues unless authorised by an appropriate manager or required by the Trust (see 7.3 below);
- make sure sensitive data is not stored on public folders;
- staff should be familiar with the security of email/internet systems;
- make sure computer discs are wiped clean correctly before being reused;
- make sure any user IDs and passwords remain confidential unless express permission has been given by management to disclose them;
- computer files should be backed up regularly and not solely saved to the hard drive.

6.5 Disclosure of Information

6.5.1 Both during and on leaving the employment of the Trust 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 Trust or its employees. In the case of any commercially sensitive information the condition applies for a period of 12 months after leaving employment.

6.5.2 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 Chief Executive Officer/Executive Principal/Head of Trust /Principal (as appropriate) 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 Trust might be prejudiced.

6.6 Preserving anonymity

6.6.1 In the event of an allegation against a teacher employed or engaged by the Trust made by a pupil at the same Trust Trust, the Trust has a duty to act in accordance with the provisions of the Education Act 2011. These provisions contain reporting restrictions preventing the publication of any material which could lead to the identification of a teacher. All employees and individuals engaged by the Trust must ensure they preserve anonymity in such cases and must not publish any material in breach of these provisions. Any employee or individual engaged by the Trust who publishes material which could lead to the identification of the employee who is the subject of an allegation of this kind may be subject to disciplinary action, up to and including dismissal.

6.6.2 For the purposes of these provisions, “publication” includes any speech, writing, relevant programme or other communication in whatever form, which is addressed to the public at large or any section of the public. For the avoidance of doubt, this includes publishing details of an allegation or other information on a social networking site which could lead to the identification of the teacher.

Such restrictions cease to apply where a teacher waives their rights by giving written consent or by going public themselves.

6.7. Media queries

6.7.1 Employees should not respond to media queries on behalf of the Trust or Trust under any circumstances. All media queries should be referred immediately to the Chief Executive Officer/Executive Principal/Head of Trust (as appropriate).

7. Use of computers, email and the internet

The email system and the internet/intranet can be 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 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.

Those using their own personal computer or equipment for Trust purposes must only do so where this has been authorised by management. Whilst using their own computer for Trust purposes, employees must do so responsibly and to comply with all applicable laws, policies and procedures, including the provisions set out in this Code. Employees should not bring their own computer or equipment onto Trust premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer/equipment must be kept securely (at the risk of the employee) and security protected so that it cannot be accessed by pupils at the Trust Schools. Any personal use of such equipment must be restricted to an employee’s break times or outside their normal working hours and must not impact on their duties in any way. Any personal equipment which has been authorised in Trust Schools must have adequate virus protection to protect Trust systems.

Computers and laptops loaned to employees by the Trust are provided to support their professional responsibilities and employees must notify their employer of any significant

personal use (see 7.1 below). Reasonable access and use of the internet/intranet and email facilities is also available to recognised representatives of professional associations' i.e. union officers.

Employees must not use Trust equipment or property for personal gain or fraudulent, malicious, illegal, libellous, immoral, dangerous, offensive purposes. Employees should not undertake IT related activities that are contrary to the 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 Trust's computers is not permitted.

7.1 Personal Use

7.1.1 The 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 Trust's operation of computing facilities or email services;
- does not interfere with the user's employment or other obligations to the Trust;
- does not interfere with the performance of professional duties;
- is of a reasonable duration and frequency;
- is carried out in the employees break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the Trust;
- does not bring the Trust and its employees into disrepute.

Such use must not be for:

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

7.1.2 Use of email and internet at home

Access to the internet from an employee's home using a Trust owned computer or through

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 Trust's computer system or use the Trust's computer facilities, without the formal agreement of their line manager.

7.2 Security

7.2.1 The 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.

7.2.2 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.

7.2.3 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 Trust can be sued for libel;
- reporting immediately to IT units when a virus is suspected in an email.

7.3. Privacy

7.3.1 The Trust respects users' 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 Trust's policy has taken place;
- when there are emergency or compelling circumstances.

7.3.2 The 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. Employees will also be notified of what information will be recorded and retained, and for how long, and who will have access to the information. If monitoring takes place, the Trust will also notify

employees of how such information will be used, which will include using such information for disciplinary purposes where applicable. Employees may make representations about any such monitoring,

Monitoring will be reasonable and in accordance with Data Protection and Human Rights obligations.

7.3.3 Employees should not have any expectation of privacy to his or her use of the Trust systems (including but not limited to networks/servers/internet usage/networks/wi-fi). The 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.

7.3.4 Use of the employee's 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. The employee's personal file area is disk space on the central computer allocated to that particular employee. Because it is not readily accessible to colleagues it should not be used for the storage of documents or other data that should be open and available to the whole staff or wider Trust community.

7.3.5 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.

7.4. Email/IT Protocols

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

7.4.1 Users must:

- within working hours, 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;
- 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 (known as 'flaming'), 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 or tamper with other people's accounts and files;
- not use their own equipment to connect to the Trust's 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 in a Trust or with children.
- Ensure that pupils are not exposed to any inappropriate images or web links whether on Trust owned computers or on their own computer/equipment used for Trust purposes (where this has been authorised). 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;
- use unsecured disks/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/intranet 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 themselves 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.

7.4.2 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 Principal/Head of School. Global sends (send to everybody in the Global address book) are prohibited;

7.5. Data Protection

7.5.1 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 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.

7.5.2 As data controller, the 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.

7.5.3 In order to comply with its duties under the Human Rights Act 1998, the 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 Trust's wider interests. In drawing up and operating this policy the Trust recognises that the need for any monitoring must be reasonable and proportionate.

7.5.4 Auditors (internal or external) are able to monitor the use of the 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.

8. Social Networking

The purpose of this policy is to ensure:

- that the Trust is not exposed to legal and governance risks;
- that the reputation of the Trust is not adversely affected;
- that users are able to clearly distinguish where information has been provided via social networking applications, that it is legitimately representative of the 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, Bebo, Myspace,
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter.

8.1 Access to Social Networking Sites

NB - if the Trust makes the decision to put a complete block on social networking sites at work , it cannot stop individuals using social networking sites at home in their own personal time, therefore all employees need to understand the implications of inappropriate and improper use of social networking sites at home in their own personal time that may result in disciplinary action being taken.

The following permissions are given in respect of social networking applications:

Restricted access for work purposes only, where explicit permission has been given by the Chief Executive Officer/Executive Principal/Head of School

8.2 Trust managed social networking sites

This may include internal forums for staff and outward facing forums for Trust activities/clubs etc.

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 Trust/ purposes. To assist with this, all employees must adhere to the following requirements:

- only use an official (i.e. 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 Trust and Academy's logos and other branding elements should be used where appropriate to indicate the Trust's support. The Trust and Academy's logos should not be used on social networking applications which are unrelated to or are not representative of the Trust's official position;
- employees should identify themselves as their official position held within the 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 Trust– the general rules on internet/email apply;

- employees 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 matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religious or other matters;
- employees should be aware that sites will be monitored.

8.3 Personal social networking sites

All employees of the Trust, individuals engaged by the Trust or individuals acting on behalf of the Trust from third party organisations should bear in mind that information they share through social networking applications, even if they are on private spaces, may still be the subject of actions for breach of contract, breach of copyright, defamation, breach of data protection, breach of confidentiality, intellectual property rights and other claims for damages. Employees must therefore not publish any content on such sites that is inappropriate or may lead to a claim, including but not limited to material of an illegal, sexual or offensive nature that may bring the Trust or the local authority into disrepute (see Appendix B for examples of such content).

Employees using social networking sites must also operate at all times in line with the Trust's Equality and Diversity policy, failure to do so may lead to disciplinary action, up to and including dismissal.

Social networking applications include, but are not limited to, public facing applications such as open discussion forums and internally-facing applications, (i.e. e-folio) regardless of whether they are hosted on Trust networks or not. The Trust expects that users of social networking applications will always exercise due consideration for the rights of others and that users will act strictly in accordance with the terms of use set out in this code.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the 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 Trust, any of its employees or any third party's reputation may amount to misconduct or gross misconduct which could result in disciplinary action, up to and including dismissal. Employees must not use social networking sites for actions that would put other employees in breach of this policy.

Employees should not use personal sites for any professional activity or in an abusive or

malicious manner. The 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 Trust or put it at risk of legal action.

8.3.1 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 Trust into disrepute.

8.3.2 Posting inappropriate comments

It is totally unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the 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.

8.3.3 Social interaction with pupils (past and present)

Employees should not engage in conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years. This would also apply to individuals who are known to be vulnerable adults. 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 Trust in a social setting and by communicating with them on social networking sites, is tantamount to the same. Individuals working in the Trust should ensure that personal social networking sites are set at private and that pupils are never listed as approved contacts.

Individuals working in the Trust should not use or access social networking sites of pupils.

8.3.4 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.

8.3.5 Reporting breaches of this code

Anyone who becomes aware of inappropriate postings on social networking sites must report it to their line manager straight away. The line manager will then follow the disciplinary

procedure where appropriate. 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 code of conduct, then that employee may be subject to disciplinary action up to and including dismissal.

Should an employee become aware of an underage person using social networking sites, (Facebook and Bebo have set it at 13 years and MySpace have set it at 14 years), then they should report this to the site operator and if that child is at their particular Trust, then this should also be reported to their line manager.

8.4 Cyber bullying

The Trust will not tolerate any form of cyber bullying by employees. Any such behaviour will result in disciplinary action, up to and including dismissal. Cyber bullying may include but is not limited to:

- Offensive emails including joke emails which may offend other employees
- Email threats
- Leaving offensive or inappropriate comments on blogs or networking sites
- Offensive comments sent by text, email or posted on social networking sites
- Sharing another person's details/personal information online without appropriate consent

Employees who feel they are the subject of cyber bullying must notify their line manager at the earliest opportunity.

9. Use of Mobile Telephones

9.1 Employees are required to ensure mobile telephones are switched off/switched to silent during teaching hours, unless a phone is being used for educational purposes. Employees are not permitted to use their mobile telephones during teaching hours, and must ensure they are stored securely and are not accessible by pupils at any time.

9.2 Employees are not permitted to contact pupils by telephone, text message or by sending picture messages using their mobile telephone or divulge their telephone number to pupils under any circumstances/unless given express permission by their line manager.

9.3 Employees provided with a mobile telephone to carry out their duties must ensure they only use the mobile telephone for the purposes agreed with their line manager. Any unauthorised usage must be reimbursed to the Trust and/or may be the subject of disciplinary action.

9.4 Any urgent phone calls or messages must be directed to the office who will notify employees immediately. Employees who need to use their mobile telephone to make or receive an urgent call during teaching hours must obtain prior authorisation from management to do so.

10. Relationships

10.1 Trust Board or Local Governing Committee proceedings

There are restrictions on trustees and governors or persons taking part in proceedings of the Trust or their committees (" a relevant person") under the School Governance (Roles, Procedures and Allowances) Regulations 2013 (Regulation 16 and Schedule 1)

The Regulations require that they must disclose his or her interest, withdraw from the meeting and not vote on the matter in question:

- if there is a conflict of interest between the interests of a relevant person and the interests of the Trust Board/Local Governing Committee,
- where a fair hearing is required and there is reasonable doubt about the relevant person's ability to act impartially; or
- where they have pecuniary interest, (for example contracts) or if a relative (including spouse) living with them has pecuniary interest.

10.2 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 Trust Board and, where applicable, the local authority.

10.3 Contracts

10.3.1 All relationships of a business or private nature with external contractors, or potential contractors, must be made known to Trust Board and/or Local Governing Committee, as appropriate. Orders and contracts must be in accordance with standing orders and financial regulations of the Education Funding Agency and the Trust. No special favour should be shown to businesses run by, for example, friends, partners or relatives in the tendering process. No part of the local community should be discriminated against.

10.3.2 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 Trust Board or

Local Governing Committee, as appropriate.

11. 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 without the express permission of the Chief Executive Officer or Trust Board, as appropriate. There are occasions when children, young people or parents wish to pass small tokens of appreciation to adults e.g. on special occasions or as a thank-you and this is acceptable. It is inappropriate to receive gifts on a regular basis or of any significant value. Employees may not give any gift to someone from whom they expect to receive any favour in their official capacity.

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 Chief Executive Officer or Trust Board, as appropriate.

Employees should always consider any particular sensitivity around accepting hospitality from an organisation that may be affected by decisions taken by the Trust Board.

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 Guidance for Safer Working Practice for those working with Children and Young People in Education Settings (Section 4) for gifts in respect of pupils.

12. Close personal relationships at work

Situations arise where relations, or those in other close relationships, may be employed at the 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 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.

12.1. Management

12.1.1 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 Chief Executive Officer/Executive Principal/Head of School (as appropriate) would need to identify another individual to undertake the particular responsibility, so that a 'conflict of interest' situation is avoided.

12.1.2 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 Trust

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

12.1.3 Employees should discuss confidentiality with their Chief Executive Officer/Executive Principal/Head of School/line manager (as appropriate), any relationships with an applicant.

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

12.1.5 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.

12.2. Impact

12.2.1 It may be appropriate to employ someone to work in a team with someone with whom 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.

12.2.2 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 the Chief Executive Officer/Executive Principal/Head of School/line manager/other manager or Trust Board in the case of Chief Executive Officer.

12.3 References

12.3.1 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.

12.3.2 Personal or colleague references should not be provided on headed paper. References on behalf of the employer should be cleared and signed by the Chief Executive Officer/Executive Principal/Head of School, as appropriate .

13. Dress code

Standards of dress and personal presentation are relevant to all employees. Whether or not there is anything in writing, minimum standards of personal presentation will be expected and an employee who is unacceptably dressed in a consistent manner can be subject to disciplinary action. In general, standards of dress should be smart, fit for purpose and portray a favourable impression of the Trust.

A dress code should reflect the culture and image of the Trust. The Head teacher is entitled to apply their discretion in determining the image of the Trust, including the personal presentation of staff, especially if they are in a position of authority, projecting an appropriate image to pupils, parents and members of the public.

There is a wide range of roles within a Trust undertaking vastly different responsibilities and activities. There will be different expectations about the appropriate way employees should dress. The policy should be as non-specific as possible and should indicate expectations

overall and not garment by garment. A dress code requiring smart appearance, with non-binding examples of suitable dress, is less likely to fall foul of claims of discrimination. The dress code should not be unreasonably restrictive for one sex, ethnic minority or religion and be flexible enough to take account of health and disability issues. The line manager will need to consider the health and safety requirements of the role held by an individual for example a caretaker would be required to wear personal protective equipment when undertaking any manual duties and PE staff may need to wear sportswear.

There may different rules for out of Trust activities (non-pupil days, summer fairs etc) but in any case dress should be such that:

- *is not likely to be viewed as offensive, revealing, or sexually provocative*
- *does not distract, cause embarrassment or give rise to misunderstanding*
- *is absent of any political or otherwise contentious slogans*
- *is not considered to be discriminatory and or culturally insensitive*

Any staff member with tattoos or body piercings should ensure that these are not visible.

14. Neutrality

14.1 Employees serve the community as a whole. It follows they must serve all members of the 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.

15. Use of financial resources

15.1 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 Trust or the Education Funding Agency. They must also observe the Education Funding Agency's financial regulations and Trust's financial regulations.

16. Sponsorship

16.1 Where an outside organisation wishes to sponsor or is seeking to sponsor a 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 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.

17 Trust Property and personal possessions

17.1 Employees must ensure they take care of Trust property at all times. If employees are found to have caused damage to Trust property through misuse or carelessness this may result in disciplinary action.

17.2 Employees are responsible for the safety and security of their personal possessions while on Trust premises. The Trust will not accept responsibility for the loss or damage of personal possessions.

Appendix A – 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's 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 Trust's 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 peoples e-mail.

Appendix B - 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 Trust or colleagues may entitle the Chief Executive Officer/Executive Principal/Head of School/line manager (as appropriate) to decide that this term has been broken. Such conduct would be subject to the Trust's 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 Trust, such conduct would be subject to the Trust's disciplinary procedure and could lead to the employee's dismissal.

3. Discrimination

The Trust's 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 claims can occur via emails, If an employee places discriminatory material about another employee, a member of the Trust Board, Local Governing Committee, parents, children, young people, and vulnerable adults, this could amount to bullying or harassment of that individual.

The 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 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 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 a Trust is aware of this and fails to investigate there may be liability for personal injuries in the law of negligence.

Appendix C – Whistleblowing Policy

Public Interest Disclosure Act 1998

1. Introduction

1.1 The Public Interest Disclosure Act 1998 ("the Act") protects workers and employees from detrimental treatment or dismissal as a consequence of disclosing information about unlawful actions of their employer or information about the conduct or behaviour of employees, volunteers or others associated with the operation and organisation of the Trust. This is known as "whistleblowing". The protection applies to employees, volunteers, agency and contract workers. The Trust is committed to creating an open and supportive environment where individuals feel able to make a disclosure and feel confident in the process that will be followed. This policy sets out how disclosures can be made and how they will be handled. All disclosures will be treated consistently and fairly.

Employees who have a role involving finance should also have regard to the Financial Regulations document for their Trust which includes a Whistleblowing Policy containing specific provisions relating to financial issues.

1.2 If an employee/worker makes a disclosure it must concern one of the 6 types of "qualifying disclosure" specified in the Act to be protected. These are where there has been or is likely to be:

- A breach of any legal obligation;
- a miscarriage of justice;
- a criminal offence;
- a danger to the Health and Safety of any individual;
- damage to the environment; and,
- deliberate concealment of information about any of the above

The employee/worker raising the concern must reasonably believe they are doing so in the public interest. This means that personal grievances and complaints are not usually covered by this policy and should be dealt with under the Grievance Procedure.

1.3 Concerns should normally be raised initially with the employee's line manager. If a concern is raised verbally it should be followed up in writing wherever possible. However, where the complaint relates to the employee/worker's line manager, the complaint should be brought to the attention of a more senior manager, the Chief Executive Officer/Executive Principal/Head of School, as appropriate, or the Local

Governing Committee. In the case of the Chief Executive Officer, the Trust Board.

2. Raising concerns

2.1 Where having raised a concern informally and the employee/worker has a genuine belief that the Trust has failed to take appropriate action or the employee/worker considers the informal process is inappropriate and wishes to raise the matter formally, they may report their concern to the Local Governing Committee or in exceptional circumstances to the Education Funding Agency or to a prescribed body. (A prescribed body is an organisation, normally with some regulatory function (for example the Health and Safety Executive), which is prescribed by the Secretary of State for the purposes of the Act who an individual may make a protected disclosure to. Any such disclosure to a prescribed body will qualify for protection under the Act. A list of prescribed bodies is available at the following link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360648/bis-14-1077-blowing-the-whistle-to-a-prescribed-person-the-prescribed-persons-list-v4.pdf

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

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

2.4 If the concern/complaint relates to the safeguarding of children (including concerns about other colleagues/works) and the employee/worker considers the informal process is inappropriate and/or wishes to raise the matter formally, they may report their concern to the to the Trust Board or they should contact their Local Authority Designated Officer (LADO) using the Duty Line – **03330 139 797**.

3. Action by recipients of disclosures

3.1 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/worker 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 Local Governing Committee, as appropriate.

Once a disclosure has been made, the line manager/Governor responsible for handling the grievance may ask the whistle-blower to attend a meeting to gather all the information needed to ensure a clear understanding of the situation. Where a meeting is held, the whistle-blower may be accompanied by a trade union representative or work colleague if they wish and where possible the dates/times will be agreed to facilitate this.

Requests to be accompanied must be clearly communicated to the Trust allowing adequate time for the Trust to deal with the companion's attendance at the meeting. The request should be made in advance of the meeting providing the name of the companion and whether they are a fellow worker or trade union official or representative.

3.2 Where complaints are received from members of the public, the Trust's formal complaints procedure must be followed, unless the complaint relates to the specific conduct or performance of an individual employee/worker in which case the Disciplinary Procedure may need to be instigated.

3.3 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.

3.4 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 Trust's auditors and/or the police. This should normally be agreed initially by the Trust Board who should, in turn, and where appropriate, keep the Education Funding Agency informed in view of any possible implications concerning public monies. Advice may be sought from the Trust's legal advisers before involving the police in any such internal complaint or allegation.

3.5 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.

3.6 All disclosures will be handled by the Trust in a timely manner. The timescales for

handling disclosures will differ depending on the nature of the disclosure made but all disclosures (whether formal or informal) will be acknowledged by the Trust within five working days. The timescales for any further steps in the process will be notified to the whistle-blower when the disclosure is acknowledged.

4. Protecting 'whistle-blowers' and complainants

4.1 Whistle-blowers are protected by the Act from suffering a detriment or dismissal as a result of making a protected disclosure which they reasonably believe is in the public interest.

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 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.

Where a whistleblower remains anonymous the Trust will not ordinarily be able to provide feedback to the whistleblower and any action taken as a result of an anonymous disclosure may be limited. The Trust will take all appropriate steps to investigate such a disclosure in line with the level of information provided. If an anonymous whistleblower wishes to seek feedback from the Trust an appropriate anonymised email address should be provided.

4.2 If an individual 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 Trust will take all reasonable steps to prevent/address such harassment or victimisation.

4.3 Whether or not work relationships suffer in this way it may well be that 'whistle-blowers' 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 an employee receives a complaint about him/herself?

5.1 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 employees/workers should inform their line manager or Local Governing Committees in the case of Executive Principal/Head of School, or the Trust Board in the case of the Chief Executive Officer – even if they believe or know the complaint to be groundless or unjustified.

5.2 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 advisable.

6. Malicious allegations

6.1 If, following appropriate investigation, it is considered that an employee has made a malicious allegation without real substance and/or which could not be reasonably considered to be in the public interest, this will be taken as a most serious matter and may potentially lead to disciplinary action in line with the Trust's disciplinary procedure.

6.2 Where other individuals engaged by the Trust make a malicious allegation, the Trust will investigate the allegation thoroughly and take appropriate action, which may include terminating the contract/arrangements with the individual.

This document is issued by:
EES for Schools, Education HR service

You can contact us in the following ways:

By telephone:
033301 39810

By email:
educationHR@EESforSchools.org

By post:
EES for Schools,
Education HR,
Seax House,
Victoria Road South,
Chelmsford,
CM1 1QH

Visit our website:
www.EESforSchools.org