
STAFF CODE OF CONDUCT

Ready
Ready

Respectful
Respectful

Safe
Safe

SEPTEMBER 2023
THE MILL ACADEMY TRUST

Staff Code of Conduct

Introduction

All adults who work in schools must act professionally and create an environment that secures the safety and well-being of children and young people and the best outcomes for them. This relies on effective interactions and good relationships between adults and children. People who work with children and young people can be vulnerable and The MILL Academy Trust Code of Conduct provides advice and guidance to ensure that staff are aware of appropriate, professional behaviour. It also gives clear advice on what could be considered to be unwise behaviour or even misconduct. Our Code of Conduct aims to protect the safety and well-being of both children and all staff who work in the Trust.

Purpose of Guidance

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. This guidance provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities. The guidance aims to:

- keep children safe by clarifying which behaviours constitute safe practice and which behaviours should be avoided;
- assist adults working with children to work safely and responsibly and to monitor their own standards and practice;
- set clear expectations of behaviour and practice relevant to the staff of The MILL Academy Trust;
- support employers in giving a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- minimize the risk of misplaced or malicious allegations made against adults who work with children and young people;
- reduce the incidence of positions of trust being abused or misused.

Guiding Principles

- Everyone who comes into contact with children and their families has a role to play in safeguarding children (DfE 'Keeping Children Safe in Education: Information for All Trust and College Staff, September 2023)
- The welfare of the child is paramount (Children Act 2004).
- 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.
- Staff must be responsible for their own actions and behaviour and should not conduct themselves in a way which could lead others to question their motivation and intentions.
- The same professional standards should always be applied regardless of culture, disability, gender, language, racial origin, religious belief and/or sexual identity.
- Staff should work and be seen to work in an open and transparent way.
- Any incidents that causes concern must be recorded and records kept of decisions made in accordance with Trust policy.
- Adults should continually monitor and review their practice and ensure they follow the guidance contained in this document.
- All staff should know who the **Designated Safeguarding Leads (DSL) are and they should be familiar with the Trust's Safeguarding policy and understand their role in safeguarding the well-being of children and young people.**
- **The Nolan Principles - The Seven Principles of Public Life**
The Seven Principles of Public Life (also known as the Nolan Principles) apply to anyone who works as a public office-holder. This includes all those who are elected or appointed to public office, nationally and locally, and all people appointed to work in the Civil Service, local government, the police, courts and probation services, non-departmental public bodies (NDPBs), and in the health, **education**, social and care services. All public office-holders are both servants of the public and stewards of public resources. The principles also apply to all those in other sectors delivering public services.

The seven principles are:

1. Selflessness

Holders of public office should act solely in terms of the public interest.

2. Integrity

Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.

3. Objectivity

Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.

4. Accountability

Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.

5. Openness

Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.

6. Honesty

Holders of public office should be truthful.

7. Leadership

Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs.

Duty of care

- When accepting a role that involves working with children all staff must accept the responsibilities and trust inherent in the role.
- All staff have a duty of care to children and must always act and be seen to act in their best interest.
- All staff whether paid or voluntary, have a duty to keep young people safe and protect them from physical and emotional harm. This is secured through the development of respectful, caring and professional relationships between staff and students and behaviour by staff that demonstrates integrity, maturity and good judgement.
- The Trust has a duty of care towards its employees and will provide a safe working environment and guidance about safe working practices in line with the Health and Safety at Work Act 1974. The act also requires employees to take care of themselves and anyone else who may be affected by their actions.
- There will be situations in which staff must make decisions or take actions where no guidance exists. Staff must always act to secure the best interests and welfare of children in their charge and will therefore be seen to be acting reasonably.

Power and Positions of Trust

- A relationship between a student and a member of staff is not a relationship of equals. Staff have a responsibility to ensure that they do not use their power to intimidate, threaten, coerce or undermine students. They should not use their status or standing to form an inappropriate relationship with students.
- Staff should avoid behaviour or situations that could be misinterpreted by others and report and record any incident that they are concerned could be misinterpreted.

- When a person aged 18 or over is in a position of trust with a child under 18, it is an offence for that person to engage in sexual activity with that child. Further guidance is found in the Sexual Offences Act 2003.

Confidentiality

- All staff have daily responsibilities that mean they will have access to confidential; information about children. Our system of confidentiality works on a 'need to know' basis and confidential information must not be discussed casually with colleagues. In some circumstances however, information may need to be anonymous. Information must never be used to intimidate, embarrass or humiliate students. Always be cautious about passing information about children to other people. Always follow GDPR and ensure you are up to date with this.
- There are circumstances in which staff **MUST** share information about a child with an appropriate person – for example when abuse or neglect is suspected, **this must be reported to a Designated Safeguarding Lead (DSL)**. If in any doubt always consult a member of the Trust or School Leadership Team. Any legal or press enquiries must always be passed to a member of the Trust Leadership Team. All staff must make sure that students understand that information that they disclose to you about any matter cannot be kept confidential and that **you cannot offer them a special confidential relationship**. If you do so you are putting yourself at risk in terms of how this could be interpreted by others.
- The Data Protection Act of 1998 governs the storing and processing of information about students and if clarification is required, consult **the DSL**.

Propriety and Behaviour

- All adults working with children and young people have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of the public in general and all those with whom they work.
- There may be times, for example, when an adult's behaviour or actions in their personal life come under scrutiny from local communities, the media or public authorities. This could be because their behaviour is considered to compromise their position in their workplace or indicate an unsuitability to work with children or young people. Misuse of drugs, alcohol or acts of violence would be examples of such behaviour.
- Conduct outside of work: unlike some other forms of employment, working at The MILL Academy Trust means that an employee's conduct outside of work could have an impact on their role. The MILL Academy Trust staff must not engage in conduct outside work which could seriously damage the reputation and standing of the Trust or the employee's own reputation or the reputation of other members of the Trust's community. Employees should be aware that any conduct that we become aware of that could impact on their role within the Trust or affect the Trust's reputation will be addressed under our disciplinary procedure. This includes use of social media even where comments are not publicly available. We therefore expect employees to make us aware immediately of any such situations that have happened outside of The MILL Academy Trust.
- Employees may take up additional employment, paid or unpaid, providing it will not create a conflict of interest, cause the Trust reputational harm or adversely affect an employee's ability to carry out their duties and responsibilities for the Trust effectively and efficiently e.g. significant increase in workload. **Private tutoring of children that attend Trust Schools is not permitted as this is in direct conflict with The Nolan Principles** (see pages1-2).

- Paid or unpaid employment includes, but is not limited to:
 - taking up employment with any employer on any type of contractual arrangement;
 - running your own business;
 - private tutoring;
 - holding directorships or trusteeships;
 - Participating or having any other interest in organisations that may be a competitor or supplier to the Trust.
- Prior permission must be sought from the School's Headteacher before taking up any additional employment.
- Carrying out public duties (e.g. jury service) does not count as additional employment.
- Employees must not use any Trust property or facilities to support additional employment and any customer must be informed that the private nature of the work is not connected with the Trust and School.
- Adults in contact with children and young people should therefore understand and be aware, that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.
- The behaviour of an adult's partner or other family members may raise similar concerns and require careful consideration by an employer as to whether there may be a potential risk to children and young people in the workplace.
- Employees must not market their private business using school/Trust data.
- Employees must not exploit their school/Trust contacts with staff/parents/families/students/carers to market or sell services/products from their own personal business enterprises for personal financial gain.

Personal Conduct, Dress and Appearance

- Staff should think carefully about revealing details of their personal lives to students, for example, the context in which it is happening, and should not discuss their personal lives within the hearing of students.
- Staff should not make, or encourage others to make, unprofessional, personal comments which scapegoat, demean or humiliate or might be interpreted as such. This includes staff to staff communications.
- No child or young person should be in or invited into the home of a member of staff unless the reason for this has been firmly established and agreed with parents/carers and the Headteacher. Staff should be vigilant in maintaining privacy and mindful of the need to avoid placing themselves in vulnerable situations
- Dress is a matter of personal choice; however, staff should ensure that their dress and appearance is appropriate to their professional role, which may be different from that adopted in their personal life. Staff should be dressed safely and appropriately so that appearance promotes a positive and professional image, and does not render them vulnerable or open to criticism. Dress should not be offensive, revealing, sexually provocative, cause embarrassment or give rise to misunderstanding.

- **Dress Code**

- Purpose
- Appearance
- Religious and cultural dress
- Implementing and review

- **Purpose**

We encourage everyone to maintain an appropriate standard of dress and personal appearance at work and to conduct themselves in a professional manner. The purpose of our dress code is to establish basic guidelines on appropriate clothing and appearance at our workplace, so that we:

- promote a positive image and staff look professional;
- respect religious, racial and gender-specific clothing requirements and those of staff with disabilities where possible;
- take account of health and safety requirements; and
- help staff decide what clothing it is appropriate to wear to work.
- Different departments may have specific requirements that result in particular clothing demands, for example, because their work raises health and safety risks. It is important that all staff dress in a manner appropriate to their working environment and the type of work they do.
- We expect staff to take a common sense approach to the dress code. Any enquiries regarding the operation of our dress code (including whether an article of clothing is suitable to wear to work) should be made to their line manager or the HR Officer.

- **Appearance**

- While working for us you represent us with students, parents and the public. Your appearance contributes to our reputation and the development of the Trust. It is important that you appear clean and smart at all times when at work
- All members of staff are supplied with an identity badge that must be worn and visible at all times when you are at work.
- With the exception of PE teachers, staff should not wear casual or gym wear to work. This includes track suits, sweat-shirts, casual or sports t-shirts or shorts, combat trousers, jogging bottoms, denim, or leggings.
- Clothing should not be dirty, frayed or torn. Tops should not carry wording or pictures that might be offensive or cause damage to our reputation. It is inappropriate to wear clothing such as cut-off shorts, crop tops, see through material or clothes that expose areas of the body normally covered at work.
- Footwear must be safe and clean and take account of health and safety considerations. Trainers, and flip-flops are not acceptable.
- Where we provide safety clothing and equipment, including protective footwear, it should be worn or used as appropriate and directed.
- Staff should not wear excessive or unconventional clothing or jewellery that could present a health and safety risk.
- Hair should be neat tidy and well groomed. Hair styles and colours which are considered extreme may be deemed as unacceptable.
- We recommend that tattoos where appropriate should remain covered at all times if they compromise a professional appearance.
- A professional appearance must be maintained at all times i.e. shirt, trousers, skirt, suits and dresses.

- **Religious and cultural dress**
 - Staff may wear religious and cultural dress (including clerical collars, head scarves, skullcaps and turbans) unless it breaches this policy or compromises the health and safety of the wearer, their colleagues or any other person.
 - Where necessary the HR Officer can disseminate appropriate information explaining cultural dress and customs.
 - Priority is at all times given to health and safety requirements. Where necessary, advice will be taken from our Health and Safety Officer.

- **Implementing and review**
 - Line Managers are responsible for ensuring that staff observe the standards set by this dress code.
 - Failure to comply with the dress code may result in action under our Disciplinary Procedure.
 - In serious cases, where an employee's appearance is, in the Headteacher's view, unacceptable the employee may be required to return home to change. In these circumstances the employee will not be paid for the duration of his/her absence from work.
 - On professional development days and holiday periods staff should wear smart casual dress. This excludes outward facing staff who continue to have direct contact with members of the public i.e. main office staff, who should continue to wear smart dress as above.
 - We will review the dress code periodically to ensure that it meets our demands, in particular with regard to health and safety of our staff and all those they deal with

Gifts, rewards, favouritism, infatuation

- It is acceptable to receive small tokens of appreciation from children or parents at Christmas or as a thank-you but staff should be careful not to accept any gift that could be considered a bribe to lead the giver to expect preferential treatment. Gifts of a significant value should not be accepted neither should gifts on a regular basis.
- It is not acceptable to give gifts to students. Any recognition given to students should be part of the Trust's rewards system and available to all students to avoid charges of favouritism.
- It is not uncommon for students to become attracted to members of staff and all staff should be aware that such situations carry a high risk of words or actions being misinterpreted. If a member of staff finds themselves or a colleague in this situation they should talk to a member of the Trust/School Leadership Team as soon as possible to allow steps to be taken to avoid hurt and distress to both parties.

Social Contact, Physical Contact

- Staff must not establish social contact with students outside of Trust to establish a friendship or to strengthen a relationship. Social contact can be misconstrued. Staff should report any situation that they feel could compromise themselves or the Trust to a School Leader.
- Staff should not give out personal details such as their home phone number, address or e-mail address to students unless the need to do so is communicated to senior staff.
- A no touch approach is not always appropriate or practical in some circumstances i.e. a young child has injured themselves or you need to break up a fight, but generally please operate a 'no touch' approach at all times. It is important to understand that well intentioned physical contact can be misinterpreted by the student or an observer. Staff must use their professional judgement at all times. Physical contact must never be secretive or represent an abuse of authority, never indulge in 'horseplay'.

- Extra caution is required when it is known that a child has suffered from previous abuse or neglect. The child might associate physical contact with these circumstances and this makes staff vulnerable to allegations of abuse.
- **Physical education and other activities requiring physical contact** – staff who teach PE or who offer music tuition will on occasions need to initiate physical contact with students in order to support the students to perform a task safely/appropriately. This must be done with the student's agreement and should be for the minimum time necessary.
- **Showers and changing** – students need privacy and respect when changing clothes or taking a shower but there needs to be an appropriate level of supervision to safeguard young people, to ensure health and safety and to make sure that bullying or teasing doesn't occur. Staff should avoid physical contact when students are changing, avoid intrusive behaviour in changing rooms, announce their intention of entering, and avoid staying in the room unless student needs dictate. Staff must not change in the same room as students or take showers with students.
- Distressed students may need comfort and reassurance and this may involve age appropriate physical contact. Staff should remain self-aware at all times and ensure that contact is not threatening, intrusive or open to misinterpretation. Always ask a member of the senior team if you are not sure what is appropriate.

Care, control and physical intervention

The circumstances in which staff can intervene with a student are covered in the 1996 Education Act. Staff may intervene to prevent a student from committing a criminal offence, injuring themselves or others, causing damage to property, engaging in behaviour prejudicial to good order and to maintain good order and discipline. Staff must have regard to the health and safety of themselves and others. In all situations where physical intervention is used, the incident and actions must be recorded.

Under no circumstances can physical force be used as a form of punishment. The use of unwarranted physical force is likely to constitute a criminal offence.

For a detailed guide on intervention consult the ***School procedure on 'Physical Intervention' and all staff should adhere to this policy.***

Behaviour Management

Students must be treated with respect and dignity and we must expect students to treat staff in the same way. Procedures for dealing with breaches of the Trust's behaviour code are covered in the '**Behaviour Blueprints**' for each school and the School's '**Attendance, Behaviour and Exclusions**' policy and these must be followed. Always try to defuse a situation before it escalates and the use of humour is often helpful. Corporal punishment is unlawful; staff should not use degrading treatment for punishment. The use of sarcasm, demeaning or insensitive comments towards students is not acceptable. It is important to inform parents of sanctions and work with them to secure the changes in behaviour required.

Sexual Contact

Any sexual contact by a member of staff towards a child or young person is illegal and this is not dependent on whether the young person consents or not. Sexual activity also includes the watching or production of pornographic material. Staff should ensure that their relationships with children and young people take place within the boundaries of a respectful, professional relationship and take care that their language or conduct does not give rise to comment or speculation. Attitudes, demeanour and language all require care and thought, particularly when members of staff are dealing with adolescent boys and girls.

One to One situations

Staff should avoid meeting students in remote, secluded areas of the school and should ensure that they can be seen when they are seeing a child on their own, for example for extra help after school or in the lunch hour. Keep the door open or sit where you can both be seen through the door pane. Staff are particularly vulnerable in areas such as counselling rooms.

Home Visits

Under no circumstances should an adult visit a child in their home outside agreed work arrangements or invite a child to their own home or that of a family member, colleague or friend. If in an emergency, such a one-off arrangement is required, the adult must have a prior discussion with a member of the School Leadership Team. In general staff other than the Inclusion Team and the Family Support Team would have no reason to visit the home. Home visits should follow the School's lone worker guidelines. The following procedures should always be adhered to:

- agree the purpose for any home visit with senior management, unless this is an acknowledged and integral part of their role e.g. social workers
- adhere to agreed risk management strategies
- always make detailed records including times of arrival and departure and work undertaken
- ensure any behaviour or situation which gives rise to concern is discussed with their manager and, where appropriate action is taken

Educational visits and after school clubs

Staff need to take particular care when supervising students in less formal situations such as after school activities, visits and residential. It is important to make sure that the less formal situation doesn't lead to situations where behaviour is misinterpreted and an inappropriate relationship established. Where overnight stays are involved and boys and girls are going, it is important that staffing reflects the gender balance of the students. All trips should be organised in line with school policy outlined in 'Educational Visits Guidance'. **Lists of students and their whereabouts should be left with the Educational Visits Co-ordinator and with the School Office** so that they can be consulted by staff at school and the list should include an estimated time of arrival back at Trust. **This includes arrangements for sports teams.** A contact mobile number for the supervising member of staff must be left with the names list.

Transporting Children

There may be situations in which staff agree to transport children in their own vehicle. It is not advisable to transport a single child in a car unless there is no alternative. If a member of staff transports children in his or her car it must be with the agreement of the parents (unless there is an emergency situation and they cannot be contacted). The car must be roadworthy and appropriately insured to include the transport of children as part of your daily job. Staff must check the detail of their individual insurance policy. No member of staff will be expected to use their own vehicle to transport children as part of Trust activities. The use of volunteer parents, in exceptional circumstances, should be discussed with the Headteacher in advance and the same safeguarding applied.

First Aid, Administration of Medication and Intimate Care

- All PE staff are first aid trained. The school provides staff training through the professional development programme. Staff should be cautious about administering first aid and in general should send for trained staff who have undergone more extensive training than the standard staff training. Wherever possible first aid should be administered with another adult present. Suitable records must be kept including accident forms, if appropriate, and parents informed as soon as possible. Always try to reassure students and explain what is happening to them.

- No medication can be kept or administered by staff. All medication must be sent to the Nurse, if applicable, or the Trust Office and administered from there by the child themselves. Permission forms have to be received from the parents/carers of any child taking medicine in school.
- Staff organising trips should make sure that a first aid trained staff member accompanies the trip and should check with the school to ensure that the member of staff has the required level of first aid training.
- Children who receive intimate care have a right to safety, privacy and dignity. A care plan must be drawn up and agreed with parents for students who require regular intimate care. Students must always be encouraged to be as independent as possible. We must always be mindful of the additional vulnerability of students with disabilities and learning needs. All guidelines and policies relating to intimate care are kept with the School Office.

The Curriculum and Sensitive Issues

- Many areas of the curriculum can include subject matter which is sexually explicit or of a sensitive nature. It is very important that this work should clearly relate to learning outcomes that can be identified in lesson plans and schemes of work to ensure that they are not misinterpreted. Curriculum leaders should provide guidance to colleagues regarding such issues. Unplanned discussion about sexual and sensitive matters can also take place and response needs careful, sensitive and professional judgement. Always talk to a School Leader staff if guidance is needed or staff are concerned by matters that have been raised in lessons. Be particularly alert to any conversations or knowledge shown that could indicate child protection concerns or are offensive to the member of staff. Always seek the support and guidance of line managers or senior colleagues. Staff must be careful to avoid a situation in which they are drawn into offensive or inappropriate discussions or could be accused of encouraging such discussion.
- All staff must abide by the school Personal Development Policy. Parents have the right to withdraw their child from all or part of sex education but not from the aspects of the science curriculum relating to the biological aspects of human growth and development.

Photography, Videos and other Creative Arts

- Staff should not take, display or distribute images of children unless they have **consent from parents or carers and the child to do so**. The Trust does not wish to reduce the use of photographs or films of Trust events in display, publicity materials or items such as in the School Newsletter, but the guidance included in this document should be adhered to.
- There is the potential for any images of children and young people to be used inappropriately. We must take every precaution to ensure that this doesn't happen whilst still making sure that we use photographic and video records as a way of celebrating success and achievement.
- Staff should be aware that past experiences could make some children feel uncomfortable about being photographed or filmed, and should be sensitive to signs of discomfort and anxiety.
- Images used for publicity purposes require the consent of the individual and parent or legal carer if under 18. This is also required for images on websites and images displayed in public places where visitors have access such as a reception area. All parents are consulted so that they can indicate if their child's photograph cannot be used in displays and publicity materials. This information is held in SIMs and staff requiring permission for use of images should check with **the Data Team** to ensure that parents have not refused consent. Such procedures are not meant to deter staff from using images but are intended to protect both children and staff.

- The following guidelines **must be adhered to at The MILL Academy Trust**
 - If photographs are used the student should not be named on websites or in places with regular public access such as a reception area.
 - If students are named, for example on displays of work, avoid use of photographs.
 - All staff must be particularly careful with material stored on school laptops. Staff should download all photographs taken on school trips and at events that include children to the network.

Safe use of the Internet and mobile phones

- Mobile phones and the use of the internet by students should be in accordance with the school's guidance on the safe use of ICT in student planners and revisited in ICT lessons. All staff should be familiar with this document and ensure that students using ICT in lessons, accessing websites and using e-mails are closely monitored.
- Under no circumstances should staff access inappropriate images in school and should be aware that if an illegal act is committed through downloading, storing or disseminating inappropriate materials involving children they are likely to be barred from working with children and young people. Accessing inappropriate materials including adults', would also be considered a very serious matter and a breach of professional standards.

Staff must not to share personal e-mail address or mobile phone numbers with students. School e-mail addresses should be used by staff at their discretion to communicate with students and/or their parents and carers. Staff should also exert extreme caution in the use of **social networking sites**, such as Facebook, which can easily be accessed by students and enable access to personal information that could be used inappropriately. Staff are strongly advised not to make comments on students' personal networking sites. Staff should always ensure that their communication with students remains at a professional and transparent level so that their intentions cannot be misinterpreted. Further guidance is available in OCC's **Simple Guidance for Staff in Education Settings on the Use of Social Network Sites** (attached).

Whistle blowing

Whistle blowing is the mechanism by which adults can voice their concerns, made in good faith, without fear of repercussion. Staff should acknowledge their individual responsibilities to bring matters of concern to the attention of senior management and/or relevant external agencies. This is particularly important where the welfare of children may be at risk. Staff should follow guidance in the Trust's **Whistle Blowing** policy.

Sharing Concerns and Recording Incidents

- All staff must be aware of the Trust's child protection procedures. This includes procedures for dealing with allegations against staff. If a member of staff is the subject of an allegation s/he is advised to contact his/her Union immediately.
- In the event of an incident occurring and an allegation being made against a member of staff, the information must be clearly and promptly recorded and reported to a member of the senior team. Early contact with parents/carers could avoid misunderstandings.
- Staff should feel confident, to discuss with either the headteacher, a member of the School Leadership Team, or their line manager, any difficulties that may affect their relationships with students or their ability to undertake their roles as effectively as is the norm so that support can be offered or action taken.
- It is essential that accurate and comprehensive records are maintained wherever concerns are raised about the conduct or actions of adults working with or on behalf of children and young people.

- In broad terms, the Trust would expect staff to report the following:-
 - Criminal offences
 - Any reasonable suspicions or evidence of physical, emotional or sexual abuse of children
 - Failure to comply with financial and legal obligations
 - Actions which endanger the health or safety of staff and students or the public
 - Actions which are intended to conceal any of the above.

It will not always be clear that a particular action falls within one of these categories and members of staff will need to use their own judgement. However, the Trust prefers that any suspicions are reported rather than ignored. If members of staff make a report in good faith, and even if it is not confirmed by investigation, they will not be liable to any disciplinary action or be otherwise disadvantaged in their employment. However, it should be noted that if they make a report maliciously, mischievously or for personal gain they may be liable to disciplinary action.

Use of Social Network Sites (OCC Guidance)

Introduction

The aim of this document is to provide some simple advice and guidance for those working with children and young people in educational settings (including volunteers) regarding the use of social Networking Sites.

The document has been produced for Governors and Head teachers of all Schools in Oxfordshire and for Senior Managers and Management Committees within the County Council's centrally managed teaching services.

Background

The use of social networking sites such as Facebook and Twitter is rapidly becoming the primary form of communication between friends and family. In addition, there are many other sites which allow people to publish their own pictures, text and videos such as YouTube and blogging sites. It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in Trust. Indeed, appropriate use of some sites may also have professional benefits.

It is naïve and out-dated however to believe that use of such sites provides a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in Trust. Difficulties arise when staff utilise these sites and they do not have the knowledge or skills to ensure adequate security and privacy settings. In addition, there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

Specific Guidance

Employees who choose to make use of social networking sites/media should be advised as follows:

- That they familiarise themselves with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended. We would recommend that as a minimum all privacy settings are set to friends only, irrespective of use/purpose
- That they do not comment or conduct or portray themselves in a manner which may:
 - Bring the Trust into disrepute;

- Lead to valid parental complaints;
- Be deemed as derogatory towards the Trust and/or its employees;
- Be derogatory towards pupils and/or parents and carers;

- Bring into question their appropriateness to work with children and young people.

- Before using any social networking site to communicate with parents, carers or children that this is agreed with the Trust's leadership team

- That they do not form on-line 'friendships' or enter into communication with parents/carers and pupils as this could lead to professional relationships being compromised.

- On-line friendships and communication with former pupils should be advised against, particularly if the pupils are under the age of 18 years

(In some cases employees in Trusts/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the Trust/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to the Specific Guidance points (above).

Safeguarding issues

Communicating with both current and former pupils via social networking sites or via other non-Trust related mechanisms such as personal e-mails and text messages can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young People in Educational Settings (March 2009)' states:

"12. Communication with Pupils (including the Use of Technology)

In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that e.safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online guidelines on acceptable user policies. These guidelines detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential."

This means that Trusts/services should:

- Have in place an Acceptable Use Policy (AUP);
- continually self-review E-Safety policies in the light of new and emerging technologies;
- have a communication policy which specifies acceptable and permissible modes of communication.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messages, e-mails, digital cameras, video, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request or respond to any personal information from the child/young person other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

This means that adults should:

- ensure that personal social networking sites are set at private and pupils are never listed as approved contacts;
- never use or access social networking sites of pupils;

- not give their personal contact details to pupils, including the mobile telephone number;
- only use equipment e.g. mobile phones, provided by Trust/service to communicate with children, making sure that parents have given permission for this form of communication to be used;
- only make contact with children for professional reasons and in accordance with any Trust/service policy;
- recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible;
- not use the internet or web-based communication channels to send personal messages to a child/young person.

Adults should be circumspect in the communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with school leaders and parents/carers. E-mail or text communications between an adult and a child/young person outside agreed protocol may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internet e-mail systems should only be used in accordance with the Trust/service's policy. Further information can be obtained from <http://www.education.gov.uk>

Recommendations

1. That this document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.
2. That appropriate links are made to this document with your school/services Acceptable Use Policy.
3. We would require that your school ICT policy makes clear the expectations on use of social network sites for staff and ideally set some boundaries around use including times of use and whose computer is used.
4. That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites.
5. The employees are informed that disciplinary action may be taken in relation to those members of staff who choose not to follow the Specific Guidance outlined above.

FAQs

Q1. Should I use my mobile phone to take photographs or video of students?

A. A school trip is a common situation where photography by pupils and staff should be encouraged, but there are potential dangers. The safest approach is to avoid the use of personal equipment and to use a school-provided item. One potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to prove that this was not the case. With school equipment there is at least a demonstration that the photography was consistent with school policy. Please also refer to the Oxfordshire Guidance of Taking Photographic Images of Children. Care should also be taken that photographs are stored appropriately. For instance to copy the photographs onto a personal laptop as opposed to a school allocated laptop might make it difficult to retain control of how the picture is used. Memory cards, memory sticks and CDs should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the school network, images should be erased immediately from their initial storage location. It is important to continue to celebrate achievements of pupils through the appropriate use of photography in communicating with parents and the community.

Q2. Should I continue to use my Social Networking site?

A. Social networking is a way of life for most young people and many adults. However, adults working with children and young people should review their use of social networks as they take on professional responsibilities. Strong passwords should be used and security settings should be applied so that you control all access to your profile. Information once published, e.g. photographs, blog posts etc is impossible to control and may be manipulated without your consent, used in different contexts or further distributed. Some adults have been caught out by posting amusing remarks about the school or colleagues, only to find them re-published elsewhere by their "friends". Even innocent remarks such as an interest in "Gang Wars" could be misinterpreted (this is actually a game). False social networking sites have been set up by pupils and staff with malicious information about staff.

Currently only a few public social networking sites authorise their members and use automated registration systems, which provide limited checks. Social networking is an excellent way to share news with family and friends. Providing the security levels have been set correctly and a strong password used, information should remain private. The danger is that few people understand profile privacy settings. The minimum age of use of a social networking website must be observed by a school, even though many pupils disregard this legal requirement. Some instant messaging applications have a facility to keep log of conversations, which could be used to protect staff in case an allegation is made. "Don't publish anything that you would not want your mum, children or boss to see, either now or in ten years' time!" "Think before you Post" (National Centre for Missing or Exploited Children)

Q3. Should I have my pupils as friends on instant messaging services?

A. Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child/young person other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Online communication provides excellent opportunities for collaborative work between groups of pupils. Monitoring or tuition, where appropriately arranged, could guide and enhance such activities.

Consideration should be given as to how this type of communication might appear to a third party. Compared with a conversation in school the use of new technology inevitably increases the potential for messages to be seen out of context or misinterpreted. If instant messaging and other social networking sites are to be used with pupils, a separate and approved account should be set up for this purpose, with the agreement of senior management. Staff need an online environment which is under their control. The first requirement is that you know who you are talking to; users must be authenticated. Schools and Local Authority should have a range of security features available to them. Logs should be available in case a false allegation is made.

Q4. What is my responsibility for the use of my school laptop at home?

A. Things that can go wrong include:

- Access to wider sites by family members, for instance a gaming site or internet shopping would increase the possibility of virus attack and identity theft.
- If another member of the family or a friend is allowed to use the computer it is difficult to ensure that the use has been appropriate, for instance that confidential information has not been accessed. Adults vary enormously in their judgements as to what is appropriate.
- If a school laptop is used at home for personal use, then it may be a taxable benefit.

Some adults may feel that access via a school laptop to adult material outside school hours and at home is appropriate. It is not; there is always a possibility that this material might be accidentally seen by a child/young person and in some cases this type of use has led to dismissal. Adults need to remember that in order for anyone else to use a school laptop in the home setting, they would need to be logged on by the person responsible for the laptop. With this in mind, think about who would be culpable in certain situations. Personal use of technology by adults has been shown to increase competence and confidence and should therefore be encouraged. Adults should refer to the school policy on the personal use of school laptops, which unfortunately varies between schools and between local authorities.

Increasingly the use of a school computers for non-professional use is being explicitly banned. "There are no circumstances that justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to the children". (DCSF Nov 2007)

Adults should therefore ensure that they must have absolute control of a school laptop allocated to their use.

Q5. What is inappropriate material?

A. Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate' and 'illegal' and 'inappropriate' but 'legal'. All staff should be aware that in the former case investigation

may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Illegal

Possessing or distributing indecent images of a person under 18 – viewing such images on-line may well constitute possession even if not saved. What is regarded as indecent would ultimately be down to a jury to decide. The police have a grading system for different types of indecent images. Remember that children may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse.

Hate/Harm/Harassment

General: There is a range of offences to do with inciting hatred on the basis of race, religion, sexual orientation etc. Individual: There are particular offences to do with harassing or threatening individuals – this includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Inappropriate

Think about this in respect of professionalism and being a role model. The scope here is enormous, but bear in mind that “actions outside of the workplace that could be as serious as to fundamentally breach the trust and confidence placed on the employee” may constitute gross misconduct.

Examples taken from real events:

- Posing offensive or insulting comments about the school on Facebook.
- Accessing adult pornography on school computers during break.
- Making derogatory comments about pupils or colleagues on social networking sites.
- Contacting pupils by e-mail or social networking without senior approval.
- Trading in sexual aids, fetish equipment or adult pornography.

Q6. How should I store personal data safely?

- A. Teachers often find it convenient to write pupil reports or staff appraisals and references at home. This may require access to confidential personal information.
- B. All personal information must be kept secure. The storage of data on a hard disk or other means is basically insecure. Making such storage secure may include password protection, encryption of data and locking the computer when not in use. Physical risks including mislaying a memory stick and laptop theft from a vehicle are all too common. Consider approaches such as not storing information unless necessary and deleting files after use. The safest long-term storage location may be the Trust network, which should have a remote backup facility.

“Information security is an integral part of the Data Protection Act 1998. You must take all reasonable steps to ensure that any personal information that you are processing is securely stored.”

All staff are strongly advised to ensure that they understand their school policy regarding data protection. National policy is developing rapidly in this area. To lose control of personal data while not complying with the school policy would be difficult to defend.

Q7. How can I use ICT appropriately to communicate with young people?

A. Young people are encouraged to report concerns, which may involve the use of new technology, e.g. a pupil might prefer to text a report about bullying, rather than arrange a face to face discussion. Friendly verbal banter between adult and pupil may not be inappropriate, but it might look very different if carried out online and might lead to difficulties if misinterpreted, forwarded or used out of context. Care in the use of automatic signatures is required e.g. “Sexylegs” is not an appropriate signature for either pupil or adult when in an educational

setting. "Adults should be circumspect in their communications with children and young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming." (DCSF Nov 2007).

Q8. As a teacher, how can I safely monitor school network use?

Filtering or recording network usage will only be effective if monitored carefully to notice and report inappropriate access or usage. Often this places a new responsibility on technical staff that they may not be trained for. This responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity.

A. It is wrong to assume that filtering and monitoring are simply technical ICT activities solely managed by the network staff. Some technical staff have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial. However technical staff should not be expected to make judgements as to what is inappropriate material or behaviour without support and supervision. Monitoring policy must be set by the senior leadership team, with set procedures to deal with incidents. The senior leadership team will require assistance from technical staff but must also involve the designated child protection coordinator and pastoral staff. A technician might, with the best of intent, check sites that a user has visited and email images to alert a colleague. Should the images prove to be illegal the technician has committed a criminal offence. A defence may be that the technician was acting within a published school procedure but staff should ensure that they receive a specific, written request to perform this work. Should an incident of concern occur there should be a clear route for immediate reporting to a School Leader. Procedures to preserve evidence by unplugging a computer or locking an account need to be in place.

Q9. Can my school limit private on-line publishing?

A. As a teacher I have been asked to sign a "Professional Conduct Agreement" that requires me to be careful when using ICT out of school. Surely that is my own business?

One situation included a teacher complaining about a parent's rudeness. Had the conversation remained private as no doubt intended, this might be regarded as simply letting off steam. However, because a social networking site was used with incorrect privacy settings, an unintended audience was included and a complaint made.

The situation is not new; teachers discussing a pupil in a shop queue might be overheard by a parent. However, the technology enables messages to be recorded, edited maliciously, used out of context, re-published or used as evidence.

The mode of use of social networking and instant messaging is often conversational with a rapid interchange of remarks. It is easy to stray from a non-school conversation between friends to professional matters and perhaps not realise the lack of control over audience.

The teacher should either be fully conversant with the security arrangements for the site in use or better avoid any information that could compromise their professional integrity.

Q10. How do I ensure safer online activity in the primary classroom?

A. Most internet use in schools is safe, purposeful and beneficial to pupils and staff. However, there is always an element of risk; even an innocent search can occasionally turn up links to adult content or imagery.

Planning and preparation is vital and the safest approach when using online material in the classroom is to test sites on the Trust system before use. For younger pupils you should direct them to a specific website or a selection of pre-approved websites and avoid using search engines.

When working with older pupils, select appropriate and safe search engines e.g. CBBC Safe Search. Appropriate search terms should be used and pre-checked. Consider carefully the age, ability and maturity of all pupils when planning online activities. When encouraging pupils to publish work online, schools should consider using sites such as "Making the News", Microsites (hosted by SEGfL), video hosting sites such as TrustsTube and TeacherTube and virtual learning environments. For image searching use sites such as Microsoft Clip Art Gallery and the National Education Network Gallery. If inappropriate material is discovered then turn off the monitor, reassure the pupils and to protect

yourself you need to log and report the URL to a school leader according to the school's E-Safety policy. Avoid printing or capturing any material.

ASCL Guidance (November 2018)

1 Protecting your professional reputation

Think carefully before posting information about your school, college, staff, pupils or parents – even if your account is private. Comments could be taken out of context and be damaging. The language you use is important as abrupt or inappropriate posts may lead to complaints.

On SNS, friends can re-post or comment on your posts which means others to whom you have not given access may view your comments.

Think about how you present yourself when you post images, when joining a group or 'liking' pages; these choices say something about you. An employer may reasonably believe that a recognisable member of staff putting an inappropriate post or image in the public domain will lower the reputation of the school or college and that could be a basis for disciplinary action. It is an implicit condition of employment that an employee owes a duty of loyalty to an employer. In addition, potential employers may also look online and you will want to consider whether your choices show you in the best light when applying for a job.

SNS are utilised by some schools, colleges and educators as a means of connecting with parents, governors and students, however, this is done via organisational or professional pages and accounts. Prior approval is also obtained from the senior leadership team, and it should be borne in mind that 13 is the minimum age requirement of most SNS.

2 Privacy settings and password security

When using social networking websites it is important that you are in control of who can see your account details and content, including photos, albums, posts, status updates and any personal information. Accounts for Twitter, Facebook and Instagram can be set to private by following these steps:

Twitter

- a) click 'profile and settings' cog icon at the top right of the Twitter homepage
- b) select 'settings'
- c) select 'security and privacy' from the left-hand menu
- d) tick 'protect my tweets' check box
- e) click 'save changes'

By selecting the 'protect my tweets' option you will be able to either accept or decline requests to follow you.

Facebook

Choosing the 'friends only' setting for every option enables a good degree of privacy. Amend your Facebook privacy settings as follows:

- a) click on 'privacy' padlock icon, at the top right of your wall
- b) review 'who can see my stuff', 'who can contact me', and 'who can look me up'
- c) select 'edit' on the drop-down menu

Instagram

By default, anyone can view your profile and posts on Instagram. You can make your posts private so that only followers you approve can see them. If your posts are set to private, only your approved followers will see them in the Photos tab of Search and Explore or on hashtag or location pages. Posts can't be set to private from a desktop computer.

To set your posts to private from the Instagram app:

iPhone or Windows Phone

- a) Go to your profile by tapping
- b) Tap
- c) Turn on the Private Account setting

Android

- a) Go to your profile by tapping
- b) Tap
- c) Turn on the Private Account setting

Updates to your privacy settings are automatically stored and do not need to be saved manually. Furthermore, you can customise each option and limit the information certain people can see. It is always useful to use the 'view as' option, to check how your profile appears to others and that the information you want to remain private or for 'friends only' is not visible to everyone. If you are not entirely sure about how to use all the settings, treat all of the information that you post as being available to everyone and act accordingly.

Friend or foe

It is a good idea to remove any friends, or customise the privacy settings for current friends, if access to your personal activity could compromise your position.

Be careful about comments you post on your friends' walls; if their profile is not set to private, your posts will be visible to everyone. Sharing content with others means that it is out of your control.

It is important, regardless of which setting you use, to assume that every post you make could be made public, as friends' settings do not guarantee privacy.

Geo-location services

There are clear implications about making sensitive information public. If using this feature on SNS, consider making your location visible only to your friends. It is also possible to disable the feature by which someone else can 'check you into' a location within your privacy settings, enabling you to control what information is shared.

Password and security

- Always use a strong password that contains a combination of upper and lower case letters and numbers and ensure that it is at least six characters long.
- Do not select the 'remember this password' option when logging on to a shared computer or device as others may later be able to access it.
- Log out after you have finished online to ensure the next user can't access your account.
- Always set a PIN or passcode on your mobile or tablet so access to your account is protected if you lose it.
- Keep anti-virus software up-to-date.

Robust security settings could prevent hacking. Further, if an employee has kept up a reasonable degree of security and if the hacker clearly had to get through numerous barriers then the exposure of material could be excusable as there was a reasonable expectation of privacy. However, if confidential information that should have remained within the organisation has been revealed, the fact the leak has been exposed is irrelevant.

3 Managing content and reporting abuse

Search your name regularly online to monitor any content about yourself. This enables you to see what others can view and provides an opportunity for you to delete anything that may compromise your reputation. Be aware of what monitoring, if any, is carried out by the school or college.

Other individuals can post images on their profile in which you are named, so think about any photos you appear in. On Facebook you can 'untag' yourself from a photo. If you do find inappropriate references to you or images of you posted by a friend online, you should contact them and ask for that content be removed. Alternatively, report directly to Facebook to request its removal, although it will be Facebook's judgement as to

whether it remains online.

In 2014 a European ruling against Google stated that the search giant must delete “inadequate, irrelevant or no longer relevant data” from its search results when requested. In theory, Google must remove links to personal information that is not relevant or in the public interest. However, the reality is that requests will still have to go through the courts resulting in a complicated battle. The information will still be available on the web, it won't be visible through a Google search.

Using email

All emails sent from a school or college account should be regarded as public, especially as a ‘data subject access’ request could be made under the Data Protection Act. Emails should always be in professional language and appropriate to being an employee. It should also be noted that where a private email account is used for issues associated with work, it has in some cases been deemed as a work account and therefore also subject to the rules of professional language and conduct.

In short, do not send an email that you would not be happy for your employer or a colleague to read. Please see the Trust's Email Protocol below:

Trust Email Good Practice Protocol

Email is an efficient and useful form of communication. Please adhere to the following guidelines to ensure its appropriate usage within the school context.

Ensure all emails always have a subject line. Emails about students should have their name and form in the subject line. All emails (both internal and external) should be clear and professional in tone, this includes spelling and punctuation. If in doubt regarding the content, ask line managers to check emails.

Staff should only use their school email account and not personal accounts when emailing students and parents. (Be aware that if your whiteboard is on, it may be displaying email content.) Please note – there can be no “reasonable expectation of privacy” with regard to the school. The MILL Academy Trust reserves the right to monitor any internal email traffic at any time.

Target your email carefully to ensure the minimum possible circulation:

What Line Managers need to see

Strategic reports/proposals, requests for advice or operational details that they need to act upon.

What Line Managers do not need to see

Operational detail that they do not need to act on, copies of routine email traffic between colleagues or colleagues and parents.

What colleagues need to see:

Requests and notices that need a response, Operational detail that they need to act on, notices regarding students they might reasonably be expected to see in their duties.

What colleagues do not need to see:

Copies of documents available through other means, emails regarding student issues they will have no involvement with.

Replying to emails

Please be aware that others may forward emails to you. Be careful to check the source of an email so that when you reply it goes to the intended recipient.

If you are away from school on a planned absence for more than two days use the out of office reply.

If you receive an offensive email it should be forward to the IT tech team for investigation. Please do not delete until after you've forwarded it.

If you choose to ignore an email, please consider whether this may impair someone else's ability to do their job. If you do need to try to resolve an issue via email, in the first email, contact ONLY the person in question and try to achieve a 'win-win' situation. "CCing" the email to other colleagues in the first instance should be an absolute rarity. Such conduct immediately raises the stakes and causes unnecessary concern in the mind of the recipient and may not help the situation.

Please do not:

Send or forward an email which is libellous, offensive, discriminatory, or contains obscene content (this encompasses anything that could be calculated to incite hatred against any ethnic, religious or other minority) nor any unsolicited promotional or advertising material, chain letters or pyramid selling schemes

Unlawfully forward confidential information or unlawfully forward copyright information.

Checking Emails

During the school day, staff should only check (or send) email when they are not teaching. Outside of the school day staff are, obviously, free to check and read their email at any time, to suit their preferred working pattern.

Sending/Replying to Emails and Teams Messages

No email or Teams message should be sent to staff between the hours of 7:00pm and 7:00am. This curfew is applied to encourage a better work-life balance and to make staff think more carefully about the emails they are sending. During the curfew, staff can draft emails and replies, but these must not be sent until 7.00am the following day. Further, staff should not email at weekends. **The weekend curfew is in effect between 7.00pm Friday and 7.00am Monday.** In terms of replies to both staff and parents, we expect that any emails are responded to within a 48 hour time period. It is highly inappropriate to chase someone up for a response to an email before 48 hours have elapsed. If a response is required urgently, it may be best to consider another form of contact rather than an email. Staff may not always monitor their email accounts during the school holidays, so they may not be able to respond within 48 hours. The Trust Policy is to avoid using personal devices at home for emails. It may be unavoidable in some circumstances, when you may have to login on your personal computer but we advise all staff to refrain from having work emails on their mobile phones/tablets or signed in on their personal computers. This is to ease the pressure on staff to constantly be replying to emails.

