CODE OF CONDUCT & ACCEPTABLE USE POLICY
September 2025

Compliance with the Code of Conduct
This code of conduct has been drawn up with a view to promoting the highest possible standards of care for the children at Milford Infants School and to reduce the risk of staff being accused of improper or unprofessional conduct in all aspects of their work. It aims to help staff work safely and professionally and to clarify what behaviour constitutes safe practice.

These expectations are set out below and should be fully observed by **all** staff, including the Headteacher and Senior Management Team who should lead by example.

Professional behaviour and conduct
We all thrive on encouragement and support. We expect everyone to find opportunities to praise, reward and encourage students and each other. We encourage everyone to play a full part in school life.

As a result of their knowledge, position and/or the authority invested in their role, all those working with children in a school or education setting are in a position of trust in relation to all pupils on the school roll.

The relationship between a person working with a child/ren is one in which the adult has a position of power or influence. It is vital for adults to understand this power; that the relationship cannot be one between equals and the responsibility they must exercise as a consequence.

The potential for exploitation and harm of vulnerable pupils means that adults have a responsibility to ensure that an unequal balance of power is not used for personal advantage or gratification.

This means that staff should not:
▪ use their position to gain access to information for their own advantage and/or a pupil's or family's detriment
▪ use their power to intimidate, threaten, coerce or undermine pupils
▪ use their status and standing to form or promote relationships with pupils which are of a sexual nature, or which may become so.

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report and record any such incident.

Staff are required to read and understand the schools Safeguarding and Child Protection policy. When child protection issues arise, staff have a duty to pass information on without delay in line with local procedures. Staff should also report incidents where they feel their actions may have been misinterpreted as soon as possible to the Headteacher or Deputy Headteacher, to include a written report of the incident.

All staff have a duty to notify the Headteacher IMMEDIATELY if they are convicted of a crime or their circumstances have changed and this affects their Childcare Disqualification Disclosure.

Relationships
Mutual respect between adults that are stakeholders of the school is essential to good school management. Close personal familiarity between individuals should be avoided as it can be detrimental to the relationship and prove embarrassing to other governors and employees.

Employees and governors will ensure that appointments are made based on merit and in accordance with the school's policies and procedures. Merit is determined based on matching the chosen candidate with a job specification and ignoring all other extraneous considerations. Employees in the course of their duties should not be involved in the appointment, pay adjustment, approval of expenses, promotion or discipline of partners, relatives or close friends.

Close personal relationships between stakeholders should not be permitted to influence decisions made and must be declared at the earliest opportunity.

Employees and volunteers at the school are required to adhere to the school's Safeguarding and Child Protection policy.

Relationships with contractors or potential contractors who are engaged or may be engaged to carry out work at the school should be made known and in the case of governors, an interest declared to the Head Teacher or Chair of Governors in accordance with the legal requirements in respect of declaring financial interest.

Political Neutrality
All employees and volunteers of the school are required to behave in a way that is politically neutral and must not allow their own personal or political opinions to interfere with the way in which they carry out their work or duty to implement the policies.

Under the Education (No 2) Act 1986 the Governing Body and the Head Teacher are required to ensure that where political issues are brought to the attention of pupils, they are offered a balanced presentation of opposing views.

Physical contact
Employees should take care that their relationships with pupils reflect the age, gender and maturity of the pupils. There will be some occasions when physical contact with students is acceptable. In general these will fall into one of the following categories:

Action to prevent harm or injury to the pupil or others
Comforting a pupil in distress
Unavoidable contact
First Aid
When pupils require assistance with intimate hygiene, staff should insist a minimum of two staff members are present except where a toilet management plan and disclaimer is in place.

Staff are **not** permitted to physically strike a student and should only restrain a student when it is necessary to protect that student or prevent an assault on another person using Team Teach strategies where possible. Staff should make reference to the school Relational Behaviour Policy. Similarly the use by staff, of derogatory language to a student is unacceptable in all circumstances.

Dress code
Staff should ensure that they are dressed decently, smartly, safely and appropriately for the tasks that they undertake and that through their appearance, they promote a positive and professional image. This also includes:

- Hair should be neat and tidy. No extreme hairstyles are allowed.
- Visible tattoos are discouraged and must be discreet.
- Jewellery should be discreet with visible piercing restricted to ears.
- Clothes should be distinguishable as work clothes, different from the clothes they would wear out of work.

Use of school premises and equipment
School equipment and premises are available only for school-related activities and should not be used for fulfilment of another job or for excessive or regular personal use, unless authorised in writing and in advance by the Headteacher.

This includes photocopying facilities, stationary, telephones and computers and the school premises. Any school equipment that is used outside of school premises, for example laptops, should be returned to the school when the employee leaves employment or upon request by the Headteacher. Staff should lead the children by example, by treating school equipment with respect, any faults or damage involving school equipment should be reported immediately.

Other employment
Employees are permitted to take up secondary employment outside the school, as long as the activity does not constitute a conflict of interest, adversely affect their primary employment at the school or exceed the legal maximum working week of 48 hours as defined by the Working Time Regulations.

Any secondary employment must be undertaken outside the working hours of the employee's normal post and employees are required to keep the Headteacher (Governing Body if the employee is the Headteacher) informed of their employment at other organisations.

Use of alcohol and illegal drugs
The taking of illegal drugs is unacceptable and will not be tolerated. All employees are expected to attend work without being under the influence of alcohol or illegal drugs and without their performance being adversely impacted by the consumption of alcohol or illegal drugs.

If alcohol or drug usage impacts on an employee's working life, the school has the right to discuss the matter with the employee and take appropriate action, having considered factors such as the school or local authority's reputation and public confidence.

Use of school communication systems and ICT
The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students/pupils learning and will in return expect staff to agree to be responsible users. Staff should be aware that school ICT systems are primarily intended for educational use, and any communication using official school systems should be professional in tone and manner using appropriate language and to respect that others may have different opinions.

The school has the right to monitor emails, phone-calls, internet activity or document production, principally in order to avoid offensive or nuisance material and to protect systems from viruses, but also to ensure proper and effective use of systems by employees.

Employees who receive inappropriate communications should inform their Headteacher or Senior Manager immediately. Staff should report any areas of concern regarding e-safety to the Headteacher, and not access the site further. Staff should embed e-safety in their work with young children.

Social Media
The availability of social media applications brings opportunities to understand, engage and communicate in new and exciting ways. However, it is also important to ensure that we balance this with our duties to the school, the community, our legal responsibilities and our reputation.

Staff are expected to use the same basic principles of professional communication online as they would through any other medium, by being courteous, discrete and by keeping children safe. The same standards of conduct **MUST** be observed in order to protect the school's reputation.

The requirements in this document apply to all members of staff at the school and the principles of the policy apply to other types of online presence such as blogs and online discussion forums.

Accessing social networking sites for personal use in work time or on work equipment is prohibited.

- Staff should not make reference on social media to the school, its employees, pupils or families. If staff adhere to this recommendation then the content of an individual's online presence should not be of concern to the school.
- School staff should not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at the school. There are obvious exceptions to this when staff members have children or close relatives within the school community.
- Staff must not post entries onto social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the school into disrepute.
- Staff should not express personal views which could be misinterpreted as those of the school or the Local Authority.
- Staff are strongly discouraged to avoid posts or comments that refer to specific or individual matters relating to the school or its stakeholders.
- Inappropriate communications involving any child in any social media, should immediately be reported to the Headteacher.
- If individuals feel aggrieved about an aspect of their work or employment, there are appropriate informal and formal avenues within the school which allow staff to raise such matters. Social networks are not the appropriate forum to raise such matters.

Data Security

All staff should have a clear understanding of the importance of Data Security, the new GDPR regulations and the schools Data Protection policy.

Anti-Fraud, corruption, theft and financial impropriety
Milford Infants' School aims to maintain high standards of probity and a good reputation. The school is committed to protecting the funds entrusted to it so that the resources can be used for their intended purpose. It is essential that the risk to the school of financial losses due to fraud, corruption, theft and financial impropriety are minimised.

The Governing Body expects Governors and its school appointed workers to demonstrate the highest standards of honesty, probity, openness and integrity in the discharge of their functions. This includes:

- compliance with appropriate legislation, Codes of Conduct, Conditions of Service, standards of appropriate professional bodies, and any other standards, guidelines or instructions which are relevant to the particular service or activity,
- Promoting an anti-fraud, anti-theft and corruption culture within the school.

The Governing Body is committed to establishing and maintaining effective arrangements to prevent fraud, corruption, theft and financial impropriety. However they recognise that these cannot always be prevented and so effective arrangements have been established to detect, report and investigate all incidents or situations where they are suspected.

The Governing Body is committed to creating and maintaining an anti-fraud, anti-theft and corruption culture which promotes the highest standards of conduct and which enables Governors, school appointed workers and other external parties to express concerns and suspicions without fear of repercussion or intimidation and in the knowledge that the information will be treated confidentially and will be investigated fully and rigorously. This includes established reporting arrangements through the School's Whistle-blowing Policy.

The Governing Body will not tolerate dishonesty on the part of any Governor, school appointed worker or any person or organisation involved in any way with the School. Where fraud, theft or corruption is detected the School will rigorously pursue appropriate action against the persons concerned including legal and/or disciplinary action, and wherever possible and deemed appropriate, will take action to recover any losses suffered.

The Governing Body are committed to working constructively with the police and other relevant agencies in relation to combating fraud, theft, corruption and financial impropriety.

Confidentiality
All employees at the school and the Governing Body come into contact with a significant volume of data and information in relation to pupils, staff, school activities and many other matters. There is an obligation to read, understand and observe the requirements of the Data Protection Policy.

Where requests for confidential information are made, the identity of the requesting party should be confirmed before passing on any information.

Staff should not give pupils or parents their own personal contacts or give a pupil a lift in their own vehicle.

Under the Data Protection Act, staff are required to collect, maintain and dispose of sensitive or personal data in a responsible manner.

All communication with the media must be directed through the Headteacher or their nominee.

Associated required reading
Data Protection Policy
E-Safety Policy
Keeping Children Safe in Education
Safeguarding and Child Protection Policy
Policy and procedure for low level concerns

I declare that I have read and understood the Code of Conduct for School Employees and the associated "Required Reading".

Name_____ Date_____

Signature_____

Staff and Volunteer Acceptable Use Policy

School Policy

This Acceptable Use Policy reflects the school e-safety policy.The school will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) applies to staff, volunteers and guests who have access to and are users of school ICT systems and to school related use of ICT systems outside of school e.g. remote access.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the School e-Safety policy
- report any suspected misuse or concerns about e-Safety to the e-Safety Leader
- monitor ICT activity in lessons, extracurricular and extended school activities
- model the safe use ICT
- refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of the school or may bring the school into disrepute (this includes personal sites)

Education

- I understand that I am responsible for the e-Safety education of pupils
- I will respect copyright and educate the pupils to respect it as well

Training

- I understand that I will participate in e-Safety training
- I understand that it is my responsibility to request training if I identify gaps in my abilities

Cyber bullying

- I understand that the school has a zero tolerance of bullying. In this context cyber bullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures

Technical Infrastructure

I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures include:

- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media (unless I have permission)
- **Passwords**
    - I will only use the password(s) given to me
    - I will never log another user onto the system using my login
- **Filtering**
    - I will not try to by-pass the filtering system used by the school
    - If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
    - I will report any filtering issues immediately
- I understand that the school will monitor my use of computers and the internet

Data Protection

- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up.
- I will use an encrypted USB stick to save work to use at home.

Use of digital images

I will follow the school's policy on using digital images making sure that:

- only those pupils whose parental permission has been given are published
- I will not use full names to identify people

Communication

I will be professional in all my communications and actions when using school ICT systems.

Email

- I will use the school provided email for all business matters
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media

- I will ask permission before I use social media for school related activities

Personal publishing

- I will follow the e-safety policy concerning the personal use of social media

Mobile Phones

- I will not use my personal mobile phone during classroom time or during contact with pupils
- I will not use my personal mobile phone to contact pupils or parents

Reporting incidents

- I will report any incidents relating to e-safety to the e-safety Leader or Headteacher.
- I will make a note of any incidents in accordance with school procedures
- I understand that in some cases the Police may need to be informed

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use ICT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

I have read and understand the full School e-safety policy and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name_____ Date_____

Signature_____

Technician Acceptable Use Policy Extension

The school ICT Technician (or person given similar responsibilities) is placed in an exceptional position of trust. Many of the duties that the Headteacher expects the ICT Technician to complete are against the Staff Acceptable User Policy of the school.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems (e.g.USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.

- User accounts will need to be created and serviced meaning that there may be access to these accounts by the ICT technician.

- Through work within the school's administration network the ICT Technician may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The ICT technicians through specific user names and password have control, (sometimes through remote workstations) to the schools network. In the past there have been examples where these powers have been abused.

Because of these areas of concern the ICT Technician should:

- be responsible for monitoring the school's network.

- be given permission to access other user's files.

- protect the users by maintaining a filter for the school.

- monitor the internet use of users within the school.

- be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the school's e-Safety Policy and AUPs.

- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.

- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties we would recommend they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet.
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- have frequent meetings with their line manger to report on any issues or trends.

As an ICT Technician (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.
Senior Member of Staff:_____

Name_____ Date_____

Signature_____

Visitor Acceptable Use Policy

Visitors should apply certain standards when using computer equipment in schools. These standards should include an awareness of Data Protection and Copyright laws.

Mobile Phones

- I will not use my personal mobile phone during classroom time or during contact with pupils
- I will not use my personal mobile phone to contact pupils or parents

Logging in

- If you use the school's equipment then request a guest log in.
- If you are using equipment that has been logged in by a member of staff always ensure a member of staff is present. Always lock the machine if they need to leave the room.

Wireless Access

- Request permission to use the wireless connection (if available) asking for an authorisation key. You may need to change proxy settings.
- Remember that bandwidth is limited so avoid intensive use such as large downloads.

Internet Access and uploading

- The schools Internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the schools normal filtering system. This might not be possible as changes to the filter can take some time.
- You are responsible for the sites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never upload and install software or updates without permission from a member of staff.

If you use your own equipment

- Make sure that it has up to date virus protection software installed.
- That you take care with trailing wires.
- That you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.

Downloading files or documents, for all files

- Make sure that the USB stick/external hard drive you use is encrypted and provided by the school; this must be returned to the school before you leave.
- Never transfer files unless you have permission.
- Make sure that you clearly state the purpose for transferring these files.

If the file contains sensitive personal data such as staff or student information

- Get permission for this in writing or by email.
- (Note: Where existing service contracts (Network/MIS support) indicate that this type of work will take place permission will not be needed).
- Use an encrypted memory stick or hard drive provided by the school.
- Transfer the file only over a secure email connection e.g. School/ College/ University email

If you take pictures, video or sound files then check

- That you have permission to capture these files.
- That the staff/children have all given their permission for these images/voices to be used.
- That if you intend to use these files in a public area (website, blog etc.) or for financial gain that you request this permission in writing or through email.

Name_____ Date_____

Signature_____