"Every Opportunity for Every Child"

Alpha Trust
Staff Code of Conduct

Alpha Trust Policy & Procedures No: AT P19

Committee:	Board of Trustees
Responsibility:	CEO
Policy reviewed:	June 2023
Approved by Alpha Trustees:	12 July 2023
Review cycle:	Two years, or sooner depending on statutory changes or guidance
Review due:	June 2025
Adopted by all Alpha Trust Academies	

CONTENTS

1. Introduction

1.1 The overriding expectation is that employees, volunteers and those engaged to work in The Alpha Trust and its constituent schools will adopt the highest standards of personal integrity and conduct both in and outside work. As role models they must behave, through their words and actions, at all times in a manner which demonstrates their suitability to work with children and which upholds the standards and reputation of the Trust and its schools.

1.2 This code of conduct provides an overall framework of the behaviours expected of individuals who work in the Trust and its schools. The code is not intended to be exhaustive and individuals should use sound professional, ethical and moral judgements to act in the best interests of the Trust, its schools, its pupils and its community.

1.3 This code should be read in conjunction with:

- other Alpha Trust and school policies and procedures
- the terms of any employment or service contracts and agreements
- relevant professional standards

2 Scope

2.1 This Code applies to all individuals employed by The Alpha Trust or those engaged by the Trust or its schools including:

- Relief/casual staff
- Supply staff
- Third parties providing services to the school (including the self-employed)
- Voluntary workers

2.2 For the purpose of elements of this code applying to all individuals set out above, they are collectively referred to as “workers”.

3 Roles and responsibilities

Board of Trustees

It is the responsibility of the Board of Trustees to establish and monitor standards of conduct within the Trust and its schools, including the establishment of relevant policies and procedures. Trustees are subject to their own Code of Conduct.

Local Governing Bodies

It is the responsibility of Local Governing Bodies to establish and monitor standards of conduct and behaviour within the school, including the establishment of relevant policies and procedures. Governors are subject to their own Code of Conduct.

Executive Principal / Principal / Headteacher / Head of School and line managers

It is the responsibility of the Executive Principal / Principal / Headteacher / Head of School and line managers to address promptly any breaches of acceptable conduct and behaviour, using informal procedures where possible but implementing formal procedures where necessary.

Employees

It is the responsibility of all employees to familiarise themselves with, and comply, with this Code. Any breaches of this Code of Conduct will be regarded as a serious matter which could result in disciplinary action, and in certain circumstances could potentially lead to dismissal.

Engaged workers/Volunteers

Engaged workers and volunteers are required to familiarise themselves, and comply, with this Code in so far is it is relevant to their role. Any breaches of this Code may result in the engagement of the worker/volunteer being terminated, in accordance with any applicable terms of engagement.

4 Reporting breaches of standards of good conduct

4.1 The Alpha Trust wishes to promote an open environment that enables individuals to raise issues in a constructive way and with confidence that they will be acted upon appropriately without fear of recrimination.

4.2 All employees, engaged workers and volunteers are expected to bring to the attention of an appropriate manager/Governing Board/Trustee any impropriety, deficiency in the provision of service or breach of policy or this Code. Where appropriate, individuals should also refer to the Alpha Trust Whistleblowing Policy which is available from the school office and the Alpha Trust website.

5. The Code of Conduct

5.1 Safeguarding and Child Protection

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

The relevant requirements specific to safeguarding and child protection are set out in:

- the Alpha Trust Safeguarding Child Protection Policy and school Child Protection and Behaviour Management Procedures.
- The Alpha Trust Management of Low-Level Concerns Policy.
- the Department for Education Statutory Guidance "Keeping Children Safe in Education" (as amended from time to time).

This is the key statutory guidance which all employees must follow and all employees and volunteers must, as a minimum, read Part 1 of that Document.

"Guidance for Safer Working Practice for those working with Children and Young People in Education Settings" issued by the Safer Recruitment Consortium sets out key expectations for adult interactions with children and young people – the full guidance is available here

In addition, individuals should be aware that it is criminal offence (s 16. Sexual Offences Act 2003) for a person aged 18 or over to have a sexual relationship with a child under 18 where that person is in a position of trust in respect of that child, even if the relationship is consensual.

Individuals should familiarise themselves with these documents, in conjunction with the body of the Code of Conduct and other relevant Alpha Trust and school policies and procedures.

Reporting safeguarding concerns

As part of our Alpha Trust-wide approach to safeguarding, we promote a culture of openness, trust and transparency in which safeguarding is a shared responsibility and our values and expectations are lived, monitored and reinforced by all staff. **In this context, everyone is expected to report any and all safeguarding concerns as soon as they arise**. This includes an expectation of self-reporting where an individual finds themselves in a situation which may be, or appear to be, compromising or where they have fallen short of expectations.

Safeguarding concerns cover a wide spectrum from serious issues where a child is harmed or at risk to lower level concerns where practice or behaviour is inappropriate, undesirable or not in keeping with usual expectations. This will include cases of inadvertent or accidental conduct and where individuals find themselves in situations which could be misinterpreted or make them vulnerable to allegations.

Who to report to

Concerns should be referred to the Executive Principal / Principal / Headteacher / Head of School (or where the concerns relate to the Executive Principal / Principal / Headteacher / Head of School, to the Chair of Governors or equivalent) or to the Designated Safeguard Lead (who will share information with the Executive Principal / Principal / Headteacher / Head of School or chair of governors). In a situation where there is a conflict of interest in reporting the matter internally, it should be reported directly to the local authority designated officer(s) (LADOs).

All issues raised will dealt with in a sensitive and proportionate manner. While there are clear procedures in place for dealing with matters of misconduct and poor performance - including procedures for dealing with safeguarding allegations against adults at the school, our objective is to protect our young people and adults, by identifying and tackling issues early and providing advice, direction and support to improve our collective and individual practice.

To support these objectives, confidential records of all reported concerns and actions taken will be kept to identify any patterns, enable monitoring and to facilitate improvement in policy and practice.

5.2 Conduct outside work

The Alpha Trust recognises and respects individuals' right to a private life without interference. However, individuals connected with the Trust and its schools must not act in a way that would bring the Trust, school, or their profession, into disrepute or that calls into question their suitability to work with children. This covers relevant criminal offences, such as violence or sexual misconduct, inappropriate behaviour such as lewd or offensive action, as well as negative comments about the Trust, the school or its community.

Workers must disclose to the school (Executive Principal / Principal / Headteacher / Head of School and in the case of the Headteacher to the Chair of Governors) immediately, any wrongdoing or alleged wrongdoing by themselves (regardless of whether they deny the wrongdoing/alleged wrongdoing), including any incidents arising from alternative employment or outside of work which may have a bearing on their employment or engagement with the Trust or school.

Employees should also refer to the expectations set out in their contract of employment and the disciplinary procedures.

In addition, any worker engaged in a post covered by the Childcare (Disqualification) Regulations 2009 ("the Regulations") must immediately inform the school of any events or circumstances which may lead to their disqualification from working in the post by virtue of the Regulations. The statutory guidance relating to Disqualification under the Childcare Act 2006 can be found at the following link:

https://www.gov.uk/government/publications/disqualification-under-the-childcare-act-2006/disqualification-under-the-childcare-act-2006#disqualification-under-the-childcare-act.

Secondary employment

The Trust does not seek to unreasonably preclude employees from undertaking additional employment but employees are required to devote their attention and abilities to their duties at the Trust / school during their working hours and to act in the best interests of the Trust and the school at all times. Accordingly, employees must not, without the written consent of the school, take secondary employment or engagement once in post. This does not apply to those whose net average weekly earnings are at or below the lower earnings limit, although they should advise the school of any secondary employment so that the employer can have regard to any responsibilities it may have in relation to the Working Time Regulations.

Secondary employment or engagement must not interfere with the performance of the employee's duties with this employer. In addition, employees should not engage in business or employment activities which are incompatible with or might conflict with the Trust or the school's interests.

5.3 Confidentiality

Confidential information can take various forms and be held and transmitted in various ways e.g. manual records (files, reports and notes), verbal discussions and electronic records. As a general rule, all information received in the course of employment or whilst volunteering/being engaged by the Trust or the school, no matter how it is received, held or transmitted, should be regarded as sensitive and confidential and must not be disclosed or divulged within or outside the Trust / school other than in accordance with the requirement of the role and/or where specific permission has been provided.

NOTE: All workers must be aware that they are obliged to disclose information relating to child protection issues and should make it clear to the individual either that confidentiality cannot be guaranteed and/or decline to receive the information and direct them to a more appropriate person e.g. the Designated Safeguarding Lead.

The Alpha Trust is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. Each school's Data Protection Policy sets out the school's commitment to data protection, and individual rights and obligations in relation to personal data.

Any actual or suspected/potential breach of data protection must be reported immediately to the school's Data Protection Officer.

Preserving anonymity

The Education Act 2011 contains reporting restrictions preventing the publication of any material which could lead to the identification of a teacher in the event of an allegation against them made by a pupil at the same school. Any individual who publishes material which could lead to the identification of the employee who is the subject of an allegation of this kind may be subject to criminal and disciplinary action, up to and including dismissal.

"Publication" includes any speech, writing, relevant programme or other communication in whatever form, which is addressed to the public at large or any section of the public. For the avoidance of doubt, this includes publishing details of an allegation or other information on a social media site which could lead to the identification of the teacher.

Media queries

Workers must not speak to the press or respond to media queries on any matter relating to the school. All media queries should be referred immediately to the Executive Principal / Principal / Headteacher / Head of School /Chair of Governors.

5.4 Use of computers, email and the internet and social media

The Alpha Trust recognises that electronic devices and media are important tools and resources in an educational context and can save time and expense.

Those using the Trust or school equipment and networks are expected to do so responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

Personal use of social media and other on-line applications which may fall into the public domain should not be such that it could bring the school into disrepute and/or call into question an individual's suitability to work with children.

Detailed expectations for each of the Alpha Trust schools are set out in the Acceptable Use Policies at Appendix A - E.

Any worker who is unsure about whether or not something they propose to do might breach that policy or if something is not specifically covered in the policy, they should seek advice from their line manager or a member of the Senior Leadership Team.

5.5 Relationships

The internal school community

All workers are expected to treat members of the school community with dignity and respect and to work co-operatively and supportively. Bullying, Harassment and Victimisation will not be tolerated (see also the Alpha Trust Grievance Procedure).

The wider community and service users

All workers have a responsibility to ensure courteous, efficient and impartial service delivery to all groups and individuals within the community. No favour must be shown to any individual or group of individuals, nor any individual or group unreasonably excluded from, or discriminated against, in any aspect of school business.

Contracts

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

Gifts and Hospitality

Workers may not accept any gift or hospitality from a person intended to benefit from their services (or those whom they supervise) or from any relative without the express permission of the school.

Where an outside organisation wishes to sponsor or is seeking to sponsor a school activity, whether by invitation, tender, negotiation or voluntarily, the sponsorship should always be related to the school's interests and never for personal benefit.

The Alpha Trust policy on gifts and hospitality is available from the school office or on the Alpha Trust website. Any breaches of this policy may lead to disciplinary action.

Neutrality

Workers must not allow their own personal, political, religious or other views and opinions to interfere with their work. They are expected to be neutral in their views in the course of their work at the school and to present a balanced view when working with pupils.

5.6 Close personal relationships at work

Close personal relationships are defined as:

- workers who are married, dating or in a partnership or co-habiting arrangement;
- immediate family members for example parent, child, sibling, grandparent;
- other relationships for example extended family (cousins, uncles, in-laws), close friendships, business associates (outside the school).

Applicants

Applicants are required to disclose on their application form if they have a close personal relationship with any person connected with The Alpha Trust or the school.

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

Workers should discuss confidentiality with their headteacher/line manager, any relationships with an applicant.

It is inappropriate for any worker to sit on an appointment panel, for those with whom they have a close personal relationship.

References

It is expected that, for those working with children, professional references, and not personal references, are sought and provided. All references provided on behalf of the school must be signed by the Executive Principal / Principal / Headteacher / Head of School (Chair of Governors for the Headteacher).

Anyone agreeing to act as a personal referee must make it clear in the reference that it is provided as a personal or colleague reference and is not a reference on behalf of the school. Personal or colleague references must not be provided on school headed paper.

Relationships at work

It is also recognised that situations arise where close personal relationships can be formed at work. Such relationships should be disclosed, in confidence, to the line manager/supervisor by the individuals concerned as this may impact on the conduct of the school.

Whilst not all such situations where those in close personal relationships work together raise issues of conflict of interest, implications can include:

- effect on trust and confidence;
- perception of service users, the public and other employees on professionalism and fairness;
- operational issues e.g. working patterns, financial and procurement separation requirements;
- conflicting loyalties and breaches of confidentiality and trust.

Open, constructive and confidential discussion between workers and managers/supervisors is essential to ensure these implications do not occur and that all parties can be protected.

No-one should be involved in discipline, promotion, pay or other decisions for anyone where there is a close personal relationship.

It may be necessary in certain circumstances to consider transferring workers that form close personal relationships at work. Any such action will be taken wherever possible by agreement with both parties and without discrimination.

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

Workers related to pupils

Any workers related to, or who are the carer of a pupil are expected to separate their familial and employment role.

Workers must not show or provide any preferential treatment to them or become involved in their education or care beyond their specific role as an employee/volunteer or their role as a parent/carer/relation. Workers may be asked to report familial relationships to the Examinations Officer in their setting.

5.7 Dress code

Adults in school are expected to adopt smart standards of dress which project an appropriate professional image to pupils, parents and members of the public. Dress should also be fit for purpose according to the specific role and activity for example appropriate dress for PE, outdoor activities etc. These standards will apply to all official school activities, including on-line/virtual teaching.

In all cases dress should be such that it:

- is not likely to be viewed as offensive, revealing, or sexually provocative;
- does not distract or cause embarrassment;
- does not include political, offensive or otherwise contentious slogans; and
- is not considered to be discriminatory and/or culturally insensitive.

Additional specific dress code requirements for each school within the Alpha Trust are set out at Appendices A to E.

5.8 Use of financial resources

Workers must ensure that they use public and any other funds entrusted to them in a responsible and lawful manner. They must strive to ensure value for money and ensure rigorous adherence to Financial Regulations.

5.9 School Property and personal possessions

Workers must ensure they take due care of Trust and school property at all times, including proper and safe use, security, appropriate maintenance and reporting faults. If employees are found to have caused damage to Trust or school property through misuse or carelessness this may result in disciplinary action.

Workers are responsible for the safety and security of their personal possessions while on Trust or school premises. The Alpha Trust and its schools will not accept responsibility for the loss or damage of personal possessions.

APPENDIX A – Colchester County High School for Girls

PART A - Staff ICT Acceptable Use Policy

Computing Facilities

The school's network of computer systems and devices is owned by the school and is made available to staff in order to support their professional work. This ICT Acceptable Use Policy has been written to protect all users – students, staff and the school community. You are responsible for professional behaviour when using the systems, all of its resources and the Internet. You are expected to be an active participant in e-Safety education, taking personal responsibility for your own and your students' awareness of the opportunities and risks posed by new technologies.

This policy applies to using school resources both on-site and off-site. You agree and accept that any computer/laptop or other ICT device loaned to you by the school is provided solely to support your professional responsibilities and that you will notify the school of "any significant personal use" as defined by HM Revenue and Customs, and seek permission for such use from either Associate Principal.

Staff should refer to the full e-Safety Policy (No44) or e-Safety Co-ordinator for further clarification or details. It is the responsibility of employees to read the latest version of the policy because technology and the law change regularly.

Staff can access the school's internal systems from outside school by using the school provided devices (Laptops / Cloud books / Tablets) that have been enabled for use with Direct Access. These devices will work the same outside of the school as if on site with the only requirement being an internet connection.

If not using a school owned device then email can be access via the website or via: https://mail.cchsg.com/owa
To access files that have been migrated to the cloud, these can be accessed through SharePoint, of which the link is found on the school website.

Logging on and Security

- You are responsible for the protection of your own network logon accounts and should not divulge passwords to anyone else.
- Always be wary about revealing your home address, telephone number, or school name on the Internet. Personal details of any adult working at the school or student at the school should not be given. (see e-Safety Policy)
- Other computer users should be respected and should not be harassed, harmed, offended or insulted. (See e-Safety policy)
- Always log off when leaving a workstation, even for a short time.
- To protect yourself and the systems, you should respect the security settings on the computers; attempting to bypass or alter the settings may put you or your work at risk. (See e-Safety policy)
- Computer storage areas are accessible by ICT Services IT Helpdesk staff who may review your files, communications and computer usage to ensure that you are using the system responsibly. (See e-Safety policy)

Use of the Network and Computer Facilities

All users must take responsibility for their own use of new technologies, making sure they use the technology safely, responsibly and legally. It is unacceptable to knowingly:

- Install any unauthorised software. Always get permission from the Network Administrator before installing, attempting to install or store programs of any type on the computers.
- Damage, disable, or otherwise harm the operation of computers, or intentionally waste resources. This puts yours and others work at risk.
- Introduce a malicious code or virus. If using removable media such as USB memory sticks do not open any files that you suspect may have been infected with a virus or malicious program. The network anti-virus programme should notify you before infected files are opened.
- Try and gain access to an unauthorised area or system.
- Use any form of hacking or cracking software / system.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence, anxiety or distress to other network users, or material which infringes copyright, or material which is unlawful.
- Use any applications or services to bring the school or its members into disrepute.

The network and computers are provided for professional and educational purposes. You may use the computers for private use in your own time providing that use does not prevent others from using resources for work purposes. (see e-Safety policy for restrictions)

You have a duty to report failings in technical safeguards which may become apparent when using systems and services.

You should protect the computers from spillages by eating or drinking well away from the ICT equipment.

Use of the Internet

Filtering software is used on the school network to prevent access to inappropriate internet sites, and to protect the computer systems. Staff should be aware that the school logs all Internet use.

Access to the Internet is provided for school activities. You may access the Internet for reasonable appropriate private use in your own time providing that use does not prevent others from using resources for work purposes. (See e-Safety policy for restrictions)

Connection to the schools wireless network is permitted only for professional/educational purposes only.

Connection with personal devices such as tablets or smartphones permitted only at the discretion of the e-Safety Coordinator, Senior Leadership Team and Network Administrator.

Only access appropriate material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive or likely to cause anxiety or distress is not permitted. (See e-Safety Policy 44 for definitions)

You should respect the work and ownership rights of people outside the school, as well as other staff or students. This includes abiding by copyright laws. (See e-Safety Policy 44 Appendix 6 for details.)

Communication and use of Email

Staff should conduct themselves with professionalism and respect in all forms of communication.

All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network. Automated software scans all email, and

removes anything which could affect the security of the computer systems, or contain unsuitable or offensive content.

Only the school email account should be used for emails which are sent on school business. You should not use a personal email account for school business. Remember that any emails sent using a school email account are sent on behalf of the school in the same way as official letters. Emails should be professional in language and tone and should not compromise the reputation of the school.

Your school email account should not be used routinely to communicate with family and close friends. Personal email accounts should be used for personal communication and also to sign up for mailing lists or online communities that are not school related.

Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, or which is bullying in nature, you should always report such messages to a member of ICT support staff and your line manager.

Your school email account should not be used in lessons or used routinely to communicate with colleagues on what could be deemed to be of a personal nature.

The sending of an email or text containing content likely to be unsuitable for children or schools is strictly forbidden.

You should regularly delete unwanted sent and received emails.

Social Media

The use of social media can enhance teaching and learning but is also used widely for social interaction. With this in mind, teachers should exercise extreme caution when using social media sites such as Facebook and ensure maximum privacy settings. (See e-Safety Policy for further guidance and clarification)

Under no circumstances should a teacher use a personal social media account in the classroom or to facilitate their lessons. It is unacceptable for a member of staff to accept a friend request from an existing student on a personal social media account. See 44c Social Media Policy for further guidance.

Use of Online/Distanced Learning programmes – Teams

When using an online learning platform like Microsoft Teams, staff at CCHSG should ensure that:

- Every Team should have 2 staff members to safeguard everyone in the Team, the additional person should ideally be a Head of Department or Year Leader
- Staff should ensure that students participating in a live stream has permission from their parents to be there. No permission - No live stream
- Staff and students should establish and follow clear ground rules of that particular Team (e.g. no speaking over each other, offering rude or silly comments, using it as a private messaging service, sharing personal details). This is likened to a teacher creating the correct climate for learning in their classroom. If live streaming, these rules need to be reiterated every session
- Students should not record, re-produce or re-distribute materials from the live stream, including taking screen shots. They will be removed from the Team immediately if found doing so and reported to the e-Safety Coordinator.

- All members of the Team participate in live streaming in neutral area, (ie, not in a bedroom or bathroom). Microsoft Teams has the capability to blur or neutralise a background should the user wish.
- Members of the Team should not disclose personal information to anyone in the stream; such as their location, date of birth or phone number to anyone on the livestream, these should always be kept private. School-allocated email addresses are the only email addresses to be used. Usernames and passwords must never be shared.
- Team members do not have to be visible –audio participation or via live chat only are also acceptable.
- All members of the Team are dressed appropriately (i.e. follows the schools normal non-uniform day dress code)

Teams should not be used on a one-to-one basis between staff and students. Remote learning on a one-to-one basis is not appropriate.

Personal Laptops / Computers / Devices

Personal laptops / computers / hand-held devices are only allowed to be used in school with permission of the Principal. Connection to the school network however must be agreed with the e-Safety Coordinator, Senior Leadership Team, Principal and IT Manager.

Disciplinary Procedures

If you breach these provisions, access to the network may be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff Code of Conduct and Disciplinary Procedures. Where appropriate, police may be involved or other legal action taken. (See e-Safety Policy for details).

ICT Services Helpdesk

Any problems or faulty equipment should be reported to the ICT Services IT Helpdesk immediately. You should not attempt to repair equipment yourself.

Mobile Device Encryption

To comply with the Data Protection Act 2018, all school owned mobile devices that could be used off site will be encrypted enabling us to ensure that all data will be kept secure if the device is lost or stolen. (A mobile device can be described as any portable device which can hold data on the local drive which would be accessible by other means if this device was lost or stolen.)

Encryption will be managed by ICT Services. No user other than a person in ICT Services may decrypt the drive on a temporary or permanent basis. Failing to adhere to this will make you liable for any data access breaches which could incur fines.

Remote Data Wipe

CCHSG staff who have access to school email through their mobile phones must accept that ICT Services will have the right to remote wipe the device to prevent any data access breaches if the device is lost or stolen. Failure to notify ICT Services in the event of a device being lost or stolen will render you personally liable for any fines incurred.

Privacy and Personal Protection

- CCHSG staff must at all times respect the privacy of other students and members of staff; this includes not taking photographs or video or sound recordings.
- Staff should not forward messages (private or otherwise) without permission from the original sender.
- Staff should not supply personal information about themselves or others, on any type of websites or within email.
- When using social media staff must keep all information about school private; especially naming the school which you work at.
- Staff must not upload any pictures or videos taken in school or that show school uniform to any social media sites including Facebook, YouTube, Instagram, WhatsApp or Snapchat

Please read this document carefully. Only once it has been signed and returned will access to the school computer network be permitted.

I have read and understand the above and agree to uphold the standards outlined within these guidelines and the e-Safety Policy.

Staff Name: _____ Signature: _____Date: _____

Policy links: AT2 Safeguarding & Child Protection Policy
A4 Behaviour, Sanctions & Rewards Policy
A5 Anti-bullying Policy
26 Code of Conduct
44c Social Media Policy

PART B - Dress Code

All staff must have a smart professional look – formal business clothing is the best guide.

Expectations

- For male staff: a suit or smart trousers, jacket/blazer, a collared shirt and tie, with top button done up.
- For female staff: a smart dress or skirt/trousers with blouse or appropriate smart top; a jacket is preferred; a formal cardigan may be worn. Skirt/dress length should be a minimum of just above the knee.
- Staff in leadership and managerial positions should routinely wear a jacket/suit.
- Smart shoes or boots should be worn. They should be suitable for a working environment – no high stilettos or flip flops for health & safety reasons. No 'Ugg boots' or similar styles; no over the knee boots. All staff are responsible for ensuring that their footwear does not prevent them from carrying out their duties or activities in a safe and effective way.
- Trainers should not be worn except for medical reasons and by PE staff.
- Staff should not wear denim, leather, leggings, short skirts, 'strappy' or low-cut tops, cut out shoulders.
- Hair style or colouring should not be extreme.
- Jewellery should be discreet.
- Facial piercings, body piercings or excessive ear piercings should not be worn and any tattoos not visible.

The Executive Principal/Associate Principals are entitled to apply their discretion in determining the image of the school/academy, including the personal presentation of staff, especially if they are in a position of authority, projecting an appropriate image to students, parents and members of the public.

APPENDIX B – The Gilberd School

PART A - Electronic Communications Acceptable Use Policy for Staff

This policy has been produced in consultation with the Essex County Council Code of Conduct Policy for Schools and Academies.

This policy should be read alongside other policies of the school, particularly:

- Electronic Communications Acceptable Use Policy for Students
- Electronic Communications Acceptable Use Policy for Visitors
- Behaviour Management Policy
- Child Protection Policy
- Data Protection Policy
- Staff Discipline and Dismissal Procedure

Revision Details	
June 2018	Changes to key contacts. Data Protection Act replaced with General Data Protection Regulations (GDPR). Additional requirements to encrypt and shred information and filming in lessons in line with the GDPR. Network manager name updated.
June 2020	Addition of remote live teaching protocols. Additional guidance on the use of avatars and bitmojis. Changes to the agreement signature protocols.
June 2022	Additional guidance on maintaining confidentiality in e-mails.
July 2023	Incorporation into Alpha Trust Code of Conduct. Minor changes to wording for consistency across schools. Reference to conducting self with professionalism and respect in all forms of communication.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

Internet

I understand that:

- All use of the school's internet and e-mail in school, away from school and at home is recorded and the logs uploaded to the school system. Your personal user area on the network may also be monitored to ensure adherence to policies and the law.
- The internet should not be used for revealing or publicising proprietary or confidential information.
- Any posting on the internet that causes damage to the school, any of its employees, students or any third party's reputation may amount to misconduct or gross misconduct which could result in dismissal.
- I must not place inappropriate images/video on the internet in any forum and must ensure that background detail (e.g. house number, street name, school) cannot identify me.
- There is restricted access to social networking platforms for work purposes only.

I will:

- Take all reasonable measures to ensure that pupils are not exposed to any inappropriate images or web links. This includes remaining in the room when students are using the internet and regularly checking screens.

- Report any accidental access to material which might be considered unacceptable immediately to my line manager and the network manager and ensure it is recorded.

I will not:

- Use the schools equipment, internet or e-mail service for unlawful activities, commercial purposes or for personal financial gain. This includes accessing, downloading, storing, creating, copying or distributing offensive material (including but not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).
- Communicate with pupils or parents using social networking sites (e.g. Facebook). Even offers of assistance to a pupil with studies via social networking sites leaves an employee vulnerable to allegations.

Copyright

I understand that the school has a Copyright Licensing Agency (CLA) Education License and this means:

- I can copy works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes and it is accompanied by a sufficient acknowledgement. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but nothing which would undermine sales of the copied information.
- If I am digitally copying or photocopying from a book I am limited to one full chapter or 5% of the book, whichever is greater.
- The audience of the copied works is limited to teachers, pupils and others directly connected with the activities of the school. This also means I cannot use copyright material on a public document (school web-site, newsletters home etc.)
- I must e-mail the office manager the title and distributor of any DVD films I intend to use (educational and non-educational). This is not necessary for short clips and documentaries used for educational purposes.

Protecting data

I understand that:

- I must ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the General Data Protection Regulations 2018. This includes the use of 'Strong' passwords and anti-virus software.
- I must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, personal computer or mobile phone) unless that storage system is encrypted and approved for such use by the school. If I am unsure on the sensitivity of data I will contact my line manager for clarification.

I will:

- Only use my work laptop when accessing SIMS data from home so as not to breach Data Protection Policy.
- Take every reasonable care to ensure students do not gain access to my passwords.
- Report immediately any accidental loss of confidential information so that appropriate action can be taken.
- Fully log off, or lock the screen before leaving my laptop or computer unattended.
- Delete or shred any personal or sensitive information that has served its purpose.

I will not:

- Allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- Store sensitive information in public folders.

School equipment (including iPads and laptops)

I understand that:

- The equipment allocated to me, and all material on it, is my responsibility and subject to random checks for appropriate usage.
- Equipment loaned to me by The Gilberd School, is provided solely to support my professional responsibilities and that I will notify The Gilberd School of any "significant personal use".
- Use of school equipment must not be for any commercial purpose or gain unless explicitly authorised by the school.
- Family members or other non-employees must not be allowed to access the academy's computer system or use the academy's computer facilities, without the formal agreement of the employee's line manager.

I will:

- Take all reasonable steps to ensure the safety and security of school ICT equipment. This includes not leaving laptops and other mobile equipment unattended. When taking equipment off site I will remove anything of a personal nature before it is returned to school.
- Protect the school network from damage by ensuring that all memory devices are virus protected and that I do not open e-mail attachments or download files from the internet that I am unsure of.
- Only download apps and other material necessary for school work.
- Take all reasonable steps to ensure the safety and security of the equipment. This includes not leaving it unattended and using the protective case provided.
- Make efforts not to intentionally waste resources. Examples of resource wastage include:
  - Excessive downloading of material from the Internet;
  - Excessive storage of unnecessary files on the network storage areas;
  - Use of computer printers to produce class sets of materials, instead of using photocopiers.

I will not:

- Use my own equipment to connect to the schools network unless specifically permitted to do so.
- Transfer Apps and other material to another unauthorised device.
- Compromise the privacy of students when taking photographs or video by leaving my iPad unlocked and unattended
- Allow a pupil to have individual use of staff iPad/laptop ICT equipment under any circumstances, for any length of time, even if supervised.
- Allow a student to have access to an individual iPad's 'restriction code' unless authorised to do so.

In the Classroom

I understand that:

- When using an Interactive white board, I will freeze/pause the whiteboard to protect the privacy of data on my computer.
- The free use of search engines by students is permitted only when a member of staff is present.
- Any filming of lessons, or parts of lessons, is only to be done with the prior agreement of the staff involved and the film is only to be stored on the school network.

Live teaching or meetings using video conferencing software

I understand that:

- I must ensure all students have their cameras off and microphones muted.
- I will make all participants aware that the session is being recorded and start recording the session as soon as the session begins. This is to safeguard both the students and staff.

- All recordings of live teaching sessions and meetings will be stored securely in a password protected area on the school network. These recordings will only be shared with individuals when there is a genuine need to do so (e.g. with students who could not access a teaching session, safeguarding concern, staff CPD).
- I cannot ask students to use their cameras unless I have written consent from parents, another member of staff or parent is present in the session and the session is being recorded.
- Staff are not to set up one to one live teaching or meetings with students unless they have written consent from parents, another member of staff or parent is present in the session and the session is being recorded.
- Students will communicate by typing using the 'conversation' window or by raising their hand. I can unmute a student's microphone if I want them to talk to ask their question.
- I must use formal language when engaging with the students as you would in the classroom.
- If only one student arrives to a live teaching session then I must explain to the student that the session will have to be rearranged, offer immediate e-mail support and then ask the student to exit the session.
- If my camera is on then I must use an appropriate background or the 'blur' background feature.
- If teaching or meeting from home and on camera I must be dressed appropriately.
- If a student is disrupting the session, or is using the conversation window inappropriately, warn the student once and on the second offence remove them from the session.
- I will ensure all the students 'hang up' at the end of the drop-in clinic and do not try to 're-join' the session.

Communicating with students, parents and colleagues

I understand that:

- I should conduct myself with professionalism and respect in all forms of communication.
- If I communicate online with pupils or parents it will only be via the school's e-mail system, VLE. web-site or video conferencing software (Microsoft Teams) **not** social network sites (Facebook etc.)
- Communication online with pupils and parents will be professional at all times. Staff should not engage in friendly "banter" style conversations with students that could be misinterpreted. Staff should use appropriate avatars or bitmojis. Staff should follow normal safeguarding procedures if they are concerned about the content or volume of online communication they receive from a student.
- I must be circumspect in personal network contact with former pupils, keeping contact with those under the age of 18 through my school e-mail account only.
- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school.

Use of Email

I understand that:

- E-mail has the same permanence and legal status as written hard copy (paper) documents and may be subject to disclosure obligations in exactly the same way. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- All school e-mails I send externally should have a signature containing your name, job title and the name of the school.
- I will only use an official (i.e. not personal) email addresses for user accounts which will be used for official purposes.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, I **must not** send confidential information belonging to the school.
- I must refer to students using their initials only in the e-mail subject line to maintain privacy. I will also refer to the location of confidential information rather than attach it to the e-mail where possible.
- Open mailboxes must not be left unattended.
- External E-mail addresses are private information and should not be shared. It is prudent to use the blind copy feature (Bcc) to ensure the privacy of addresses when sending to a 'group' or large numbers of recipients.

- E-mail 'threads' may also contain confidential information and so should be considered before forwarding, or replying to, e-mails.

I will not:

- Email sensitive or personal information about staff or students to a non-school email account. Personal or sensitive information e-mailed externally must be password protected or encrypted. Emails stored on the school email system should only be accessed by webmail or Outlook.
- Send unnecessary mass e-mails without consultation with the Head teacher. I will also ensure I do not copy others into e-mails (such as using 'Reply all') unless I am sure they need the information contained.

Privacy

I understand that:

- If I feel my privacy has been compromised by students, for example, taking pictures of me without permission or personal details being acquired online then I must report it immediately to my line manager.
- Website photographs that include students will be carefully selected and will be of a type that does not allow individual students to be identified.

I will not:

- Use my personal mobile phone or other electronic equipment to photograph or video pupils unless authorised to do so.

Further advice on all E-Safety issues can be found at; www.ceop.gov.uk, www.thinkuknow.co.uk, www.childnet.com/kia, www.teachtoday.eu. All the teaching and local government union web-sites contain useful advice on communicating safely electronically. **This policy and additional detail can be viewed on the staff X: drive in the 'Policies' folder.** Please report any technical problems immediately to IThelpdesk@gilberd.com or ring 157.

By selecting 'Yes' on the voting buttons on the e-mail accompanying this policy you are agreeing that:

- I understand that by not following these rules I may be subject to legal proceedings and the use of the school's Disciplinary Procedure. Sanctions will depend upon the gravity of misuse and could result in dismissal.
- I confirm that I have read and understood The Gilberd School's **Electronic Communications Acceptable Use Policy for Staff**.

PART B – Dress Code

Adults in school are expected to adopt smart standards of dress which project an appropriate professional image to pupils, parents and members of the public. Dress should also be fit for purpose according to the specific role and activity for example appropriate dress for PE, outdoor activities etc. These standards will apply to all official school activities, including on-line/virtual teaching .

In all cases dress should be such that it:

- is not likely to be viewed as offensive, revealing, or sexually provocative;
- does not distract or cause embarrassment;
- does not include political, offensive or otherwise contentious slogans; and
- is not considered to be discriminatory and/or culturally insensitive

APPENDIX C – The Trinity School

PART A - Electronic Communications Acceptable Use Policy for Staff

This policy has been produced in consultation with the Essex County Council Code of Conduct Policy for Schools and Academies.

This policy should be read alongside other policies of the school, particularly:

- Electronic Communications Acceptable Use Policy for Students
- Electronic Communications Acceptable Use Policy for Visitors
- Behaviour Management Policy
- Child Protection Policy
- Data Protection Policy
- Staff Discipline and Dismissal Procedure

Revision Details	
June 2018	Changes to key contacts. Data Protection Act replaced with General Data Protection Regulations (GDPR). Additional requirements to encrypt and shred information and filming in lessons in line with the GDPR. Network manager name updated.
June 2020	Addition of remote live teaching protocols. Additional guidance on the use of avatars and bitmojis. Changes to the agreement signature protocols.
June 2022	Additional guidance on maintaining confidentiality in e-mails.
July 2023	Incorporation into Alpha Trust Code of Conduct. Minor changes to wording for consistency across schools. Reference to conducting self with professionalism and respect in all forms of communication.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

Internet

I understand that:

- All use of the school's internet and e-mail in school, away from school and at home is recorded and the logs uploaded to the school system. Your personal user area on the network may also be monitored to ensure adherence to policies and the law.
- The internet should not be used for revealing or publicising proprietary or confidential information.
- Any posting on the internet that causes damage to the school, any of its employees, students or any third party's reputation may amount to misconduct or gross misconduct which could result in dismissal.
- I must not place inappropriate images/video on the internet in any forum and must ensure that background detail (e.g. house number, street name, school) cannot identify me.
- There is restricted access to social networking platforms for work purposes only.

I will:

- Take all reasonable measures to ensure that pupils are not exposed to any inappropriate images or web links. This includes remaining in the room when students are using the internet and regularly checking screens.

- Report any accidental access to material which might be considered unacceptable immediately to my line manager and the network manager and ensure it is recorded.

I will not:

- Use the schools equipment, internet or e-mail service for unlawful activities, commercial purposes or for personal financial gain. This includes accessing, downloading, storing, creating, copying or distributing offensive material (including but not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).
- Communicate with pupils or parents using social networking sites (e.g. Facebook). Even offers of assistance to a pupil with studies via social networking sites leaves an employee vulnerable to allegations.

Copyright

I understand that the school has a Copyright Licensing Agency (CLA) Education License and this means:

- I can copy works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes and it is accompanied by a sufficient acknowledgement. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but nothing which would undermine sales of the copied information.
- If I am digitally copying or photocopying from a book I am limited to one full chapter or 5% of the book, whichever is greater.
- The audience of the copied works is limited to teachers, pupils and others directly connected with the activities of the school. This also means I cannot use copyright material on a public document (school web-site, newsletters home etc.)
- I must e-mail the office manager the title and distributor of any DVD films I intend to use (educational and non-educational). This is not necessary for short clips and documentaries used for educational purposes.

Protecting data

I understand that:

- I must ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the General Data Protection Regulations 2018. This includes the use of 'Strong' passwords and anti-virus software.
- I must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, personal computer or mobile phone) unless that storage system is encrypted and approved for such use by the school. If I am unsure on the sensitivity of data I will contact my line manager for clarification.

I will:

- Only use my work laptop when accessing SIMS data from home so as not to breach Data Protection Policy.
- Take every reasonable care to ensure students do not gain access to my passwords.
- Report immediately any accidental loss of confidential information so that appropriate action can be taken.
- Fully log off, or lock the screen before leaving my laptop or computer unattended.
- Delete or shred any personal or sensitive information that has served its purpose.

I will not:

- Allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- Store sensitive information in public folders.

School equipment (including iPads and laptops)

I understand that:

- The equipment allocated to me, and all material on it, is my responsibility and subject to random checks for appropriate usage.
- Equipment loaned to me by The Trinity School, is provided solely to support my professional responsibilities and that I will notify The Trinity School of any "significant personal use".
- Use of school equipment must not be for any commercial purpose or gain unless explicitly authorised by the school.
- Family members or other non-employees must not be allowed to access the academy's computer system or use the academy's computer facilities, without the formal agreement of the employee's line manager.

I will:

- Take all reasonable steps to ensure the safety and security of school ICT equipment. This includes not leaving laptops and other mobile equipment unattended. When taking equipment off site I will remove anything of a personal nature before it is returned to school.
- Protect the school network from damage by ensuring that all memory devices are virus protected and that I do not open e-mail attachments or download files from the internet that I am unsure of.
- Only download apps and other material necessary for school work.
- Take all reasonable steps to ensure the safety and security of the equipment. This includes not leaving it unattended and using the protective case provided.
- Make efforts not to intentionally waste resources. Examples of resource wastage include:
  - Excessive downloading of material from the Internet;
  - Excessive storage of unnecessary files on the network storage areas;
  - Use of computer printers to produce class sets of materials, instead of using photocopiers.

I will not:

- Use my own equipment to connect to the schools network unless specifically permitted to do so.
- Transfer Apps and other material to another unauthorised device.
- Compromise the privacy of students when taking photographs or video by leaving my iPad unlocked and unattended
- Allow a pupil to have individual use of staff iPad/laptop ICT equipment under any circumstances, for any length of time, even if supervised.
- Allow a student to have access to an individual iPad's 'restriction code' unless authorised to do so.

In the Classroom

I understand that:

- When using an Interactive white board, I will freeze/pause the whiteboard to protect the privacy of data on my computer.
- The free use of search engines by students is permitted only when a member of staff is present.
- Any filming of lessons, or parts of lessons, is only to be done with the prior agreement of the staff involved and the film is only to be stored on the school network.

Live teaching or meetings using video conferencing software

I understand that:

- I must ensure all students have their cameras off and microphones muted.
- I will make all participants aware that the session is being recorded and start recording the session as soon as the session begins. This is to safeguard both the students and staff.

- All recordings of live teaching sessions and meetings will be stored securely in a password protected area on the school network. These recordings will only be shared with individuals when there is a genuine need to do so (e.g. with students who could not access a teaching session, safeguarding concern, staff CPD).
- I cannot ask students to use their cameras unless I have written consent from parents, another member of staff or parent is present in the session and the session is being recorded.
- Staff are not to set up one to one live teaching or meetings with students unless they have written consent from parents, another member of staff or parent is present in the session and the session is being recorded.
- Students will communicate by typing using the 'conversation' window or by raising their hand. I can unmute a student's microphone if I want them to talk to ask their question.
- I must use formal language when engaging with the students as you would in the classroom.
- If only one student arrives to a live teaching session then I must explain to the student that the session will have to be rearranged, offer immediate e-mail support and then ask the student to exit the session.
- If my camera is on then I must use an appropriate background or the 'blur' background feature.
- If teaching or meeting from home and on camera I must be dressed appropriately.
- If a student is disrupting the session, or is using the conversation window inappropriately, warn the student once and on the second offence remove them from the session.
- I will ensure all the students 'hang up' at the end of the drop-in clinic and do not try to 're-join' the session.

Communicating with students, parents and colleagues

I understand that:

- I should conduct myself with professionalism and respect in all forms of communication.
- If I communicate online with pupils or parents it will only be via the school's e-mail system, VLE. web-site or video conferencing software (Microsoft Teams) **not** social network sites (Facebook etc.)
- Communication online with pupils and parents will be professional at all times. Staff should not engage in friendly "banter" style conversations with students that could be misinterpreted. Staff should use appropriate avatars or bitmojis. Staff should follow normal safeguarding procedures if they are concerned about the content or volume of online communication they receive from a student.
- I must be circumspect in personal network contact with former pupils, keeping contact with those under the age of 18 through my school e-mail account only.
- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school.

Use of Email

I understand that:

- E-mail has the same permanence and legal status as written hard copy (paper) documents and may be subject to disclosure obligations in exactly the same way. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- All school e-mails I send externally should have a signature containing your name, job title and the name of the school.
- I will only use an official (i.e. not personal) email addresses for user accounts which will be used for official purposes.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, I **must not** send confidential information belonging to the school.
- I must refer to students using their initials only in the e-mail subject line to maintain privacy. I will also refer to the location of confidential information rather than attach it to the e-mail where possible.
- Open mailboxes must not be left unattended.
- External E-mail addresses are private information and should not be shared. It is prudent to use the blind copy feature (Bcc) to ensure the privacy of addresses when sending to a 'group' or large numbers of recipients.

- E-mail 'threads' may also contain confidential information and so should be considered before forwarding, or replying to, e-mails.

I will not:

- Email sensitive or personal information about staff or students to a non-school email account. Personal or sensitive information e-mailed externally must be password protected or encrypted. Emails stored on the school email system should only be accessed by webmail or Outlook.
- Send unnecessary mass e-mails without consultation with the Head teacher. I will also ensure I do not copy others into e-mails (such as using 'Reply all') unless I am sure they need the information contained.

Privacy

I understand that:

- If I feel my privacy has been compromised by students, for example, taking pictures of me without permission or personal details being acquired online then I must report it immediately to my line manager.
- Website photographs that include students will be carefully selected and will be of a type that does not allow individual students to be identified.

I will not:

- Use my personal mobile phone or other electronic equipment to photograph or video pupils unless authorised to do so.

Further advice on all E-Safety issues can be found at; www.ceop.gov.uk, www.thinkuknow.co.uk, www.childnet.com/kia, www.teachtoday.eu. All the teaching and local government union web-sites contain useful advice on communicating safely electronically. **This policy and additional detail can be viewed on the staff X: drive in the 'Policies' folder.** Please report any technical problems immediately to IThelpdesk@gilberd.com or ring 157.

By selecting 'Yes' on the voting buttons on the e-mail accompanying this policy you are agreeing that:

- I understand that by not following these rules I may be subject to legal proceedings and the use of the school's Disciplinary Procedure. Sanctions will depend upon the gravity of misuse and could result in dismissal.
- I confirm that I have read and understood The Trinity School's **Electronic Communications Acceptable Use Policy for Staff**.

PART B – Dress Code

Adults in school are expected to adopt smart standards of dress which project an appropriate professional image to pupils, parents and members of the public. Dress should also be fit for purpose according to the specific role and activity for example appropriate dress for PE, outdoor activities etc. These standards will apply to all official school activities, including on-line/virtual teaching .

In all cases dress should be such that it:

- is not likely to be viewed as offensive, revealing, or sexually provocative;
- does not distract or cause embarrassment;
- does not include political, offensive or otherwise contentious slogans; and
- is not considered to be discriminatory and/or culturally insensitive

APPENDIX D – Manningtree High School

PART A – ICT Acceptable Use Policy

1. Introduction

ICT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.

All members of the school community are expected to use ICT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

This policy is designed to ensure that all workers are aware of their professional responsibilities when using any form of ICT.

Failure to follow this policy may result in the withdrawal of access to school computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.

Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

2. Use of School Equipment/Networks

Computers, Mobile Phones and other devices provided by the school are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

Any appropriate and authorised electronic communication with pupils must be through official school network, channels, systems and on school equipment.

3. Communication and use of Email

Staff should conduct themselves with professionalism and respect in all forms of communication.

School business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

4. Social Networks

Social networking applications include but are not limited to:

- Blogs
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter

Where the school operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- users should identify themselves as their official position held within the school on social networking applications e.g. through providing additional information on user profiles;
- any contributions on any social networking application must be professional, uphold the reputation of the school and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;

5. Personal use of school Equipment/Networks

School equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the school's operation of computing facilities or email services;
- does not interfere with the user's employment or performance of professional duties or other obligations to the school;
- is of a reasonable duration and frequency;
- is carried out in authorised break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the school;
- is not uses to access, send, receive or store inappropriate material; and
- does not bring the school and its community into disrepute.
- Workers must notify the school of any significant personal use.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

School equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the school;
- personal financial gain;
- personal use that is inconsistent of other school policies or guidelines; or
- ordering of goods to be delivered to the school address or in the school's name.

6. Use of personal ICT equipment in school

6.1 Mobile Phones

It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time.

Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.

Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks. Any urgent phone calls or messages must be directed to the office who will notify workers immediately. Workers who need to use their mobile telephone to make or receive an urgent call during working hours should where possible obtain prior authorisation from their line manager to do so.

6.2 Other electronic devices

Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.

Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

No pictures or videos may be taken within school or at any school related activity, on personal devises.

7. Personal social networks

The school recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the school, to comply with the Code of Conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.

The school may require the removal of content it considers inappropriate.

It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the school community or any school related business on any type of social networking site.

Other posting on personal sites may also impact on the reputation of the school or the suitability/conduct of the employee for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent or inappropriate images/activities etc.

Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.

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

8. Security

The school follows sound professional practices to secure data, system programmes, email records and networks under its control.

Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:

- using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
- ensuring all devices and system access are password protected Using secured memory sticks (all laptops, memory sticks and devices used must be encrypted);
- ensuring that pupils are not exposed to any inappropriate images or web links; and
- respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

9. Privacy and Monitoring

The school respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage.

However, workers should not have any expectation of absolute privacy in his or her use of the school systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the school reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law; or school's policy has taken place;
- if the school suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the school suspects that the employee has been spending an excessive amount of time on activity which is not work related;
- where required for compliance checks e.g. auditors, data protection; or
- where there are emergency or compelling circumstances.

The school will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).

Workers will normally be notified of what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.

When monitoring emails, the school will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are permitted by the school) as such and encourage those who send them to do the same. The school will avoid, where possible, opening emails clearly marked as private or personal.

The school considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the school to continue;
- if the school suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the school understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the school suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the school); and
- if the school suspects that the employee is sending or receiving emails that are detrimental to the school or its pupils.

The school may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the school e.g. whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g. checking that the school is complying with external or internal regulations;
- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would include checking that workers are not breaching the school's policy on email and internet use; and
- ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation.

9.1 Covert monitoring

The use of covert monitoring will only be used in exceptional circumstances, for example, where the school suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.

If the school considers covert monitoring to be justified, this will only take place as part of a specific investigation and will cease when the investigation has been completed.

PART B – Dress Code

Adults in school are expected to adopt smart standards of dress which project an appropriate professional image to pupils, parents and members of the public. Dress should also be fit for purpose according to the specific role and activity for example appropriate dress for PE, outdoor activities etc. These standards will apply to all official school activities.

In all cases dress should be such that it:

- is not likely to be viewed as offensive, revealing, or sexually provocative;
- does not distract or cause embarrassment;
- does not include political, offensive or otherwise contentious slogans; and
- is not considered to be discriminatory and/or culturally insensitive

APPENDIX E – HOME FARM PRIMARY SCHOOL

PART A – ICT Acceptable Use Agreement

1. Introduction

ICT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.

All members of the school community are expected to use ICT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

This policy is designed to ensure that all workers are aware of their professional responsibilities when using any form of ICT.

Failure to follow this policy may result in the withdrawal of access to school computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.

Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

2. Use of School Equipment/Networks

Computers, Mobile Phones and other devices provided by the school are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

Any appropriate and authorised electronic communication with pupils must be through official school network, channels, systems and on school equipment.

3. Communication and use of Email

Staff should conduct themselves with professionalism and respect in all forms of communication.

School business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

4. Social Networks

Social networking applications include but are not limited to:

- Blogs
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter

Where the school operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- users should identify themselves as their official position held within the school on social networking applications e.g. through providing additional information on user profiles;
- any contributions on any social networking application must be professional, uphold the reputation of the school and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;

5. Personal use of school Equipment/Networks

School equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the school's operation of computing facilities or email services;
- does not interfere with the user's employment or performance of professional duties or other obligations to the school;
- is of a reasonable duration and frequency;
- is carried out in authorised break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the school;
- is not uses to access, send, receive or store inappropriate material; and
- does not bring the school and its community into disrepute.
- Workers must notify the school of any significant personal use.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

School equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the school;
- personal financial gain;
- personal use that is inconsistent of other school policies or guidelines; or
- ordering of goods to be delivered to the school address or in the school's name.

6. Use of personal ICT equipment in school

6.1 Mobile Phones

It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time.

Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.

Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks. Any urgent phone calls or messages must be directed to the office who will notify workers immediately. Workers who need to use their mobile telephone to make or receive an urgent call during working hours should where possible obtain prior authorisation from their line manager to do so.

a. Other electronic devices

Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.

Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

No pictures or videos may be taken within school or at any school related activity, on personal devises.

7. Personal social networks

The school recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the school, to comply with the Code of Conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.

The school may require the removal of content it considers inappropriate.

It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the school community or any school related business on any type of social networking site.

Other posting on personal sites may also impact on the reputation of the school or the suitability/conduct of the employee for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent or inappropriate images/activities etc.

Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.

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

8. Security

The school follows sound professional practices to secure data, system programmes, email records and networks under its control.

Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:

- using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
- ensuring all devices and system access are password protected and using secured memory sticks (all laptops, memory sticks and devices used must be encrypted).
- Windows account passwords must be changed in line with recommendations and will automatically expire after 119 days if not changed before. The number of days before passwords must be changed has been defined taking into account security and user accessibility. This is reviewed periodically and may change depending on security requirements.
- ensuring that pupils are not exposed to any inappropriate images or web links; and
- respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.
- Devices owned by the school and used by staff or students will be connected to the corporate wireless network. Any device not owned by the school or used by guests which requires internet access will be required to join the HFPS Guest wireless SSID. This SSID has been setup specifically to ensure all traffic is segregated from the corporate network ensuring data security.

Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

9. Privacy and Monitoring

The school respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage.

However, workers should not have any expectation of absolute privacy in his or her use of the school systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the school reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law; or school's policy has taken place;
- if the school suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the school suspects that the employee has been spending an excessive amount of time on activity which is not work related;
- where required for compliance checks e.g. auditors, data protection; or
- where there are emergency or compelling circumstances.

The school will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).

Workers will normally be notified of what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.

When monitoring emails, the school will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are permitted by the school) as such and encourage those who send them to do the same. The school will avoid, where possible, opening emails clearly marked as private or personal.

The school considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the school to continue;
- if the school suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the school understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the school suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the school); and
- if the school suspects that the employee is sending or receiving emails that are detrimental to the school or its pupils.

The school may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the school e.g. whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g. checking that the school is complying with external or internal regulations;
- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would include checking that workers are not breaching the school's policy on email and internet use; and
- ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation.

9.1 Covert monitoring

The use of covert monitoring will only be used in exceptional circumstances, for example, where the school suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.

If the school considers covert monitoring to be justified, this will only take place as part of a specific investigation and will cease when the investigation has been completed.

PART B – DRESS CODE

Adults in school are expected to adopt smart standards of dress which project an appropriate professional image to pupils, parents and members of the public. Dress should also be fit for purpose according to the specific role and activity and should enable the wearer to meet health and safety requirements. For example appropriate dress and training shoes should be worn for PE and outdoor activities etc, the wearing of closed toe shoes where there are any hazards which risk injury to feet etc.

These standards will apply to all official school activities.

In all cases dress should be such that it:

- does not include political, offensive or otherwise contentious slogans; and
- is not considered to be discriminatory and/or culturally insensitive