



Thomas Whitehead CE Academy

Online Safety Policy

- Social Media
- Acceptable Use Policy

Policy type	Local Academy Policy
Reviewal timeframe	Annual
Author/Responsible Officer	Della Mitra Deputy Headteacher
Board to be ratified	Local Governing Board
Approved by	Natasha Chiswell
Signature	N Chiswell
Date of ratification	April 2026
Date of next review	September 2028

This is a Church of England Academy and in common with all church schools, aims to provide the best possible education for each of its pupils within the context of a caring, Christian community; enabling our children to become wise, hopeful, aspirational and live well together with dignity and respect.

As a Values school, we are committed to reflecting the essence of Christian Values within this policy.

Introduction

Thomas Whitehead CE Academy is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. All children have the right to an education which offers them the best opportunities to work hard, be happy and to make good progress. We recognise that all children have the right to feel safe and secure and that all staff are here to create the appropriate environment and opportunities for this to happen.

Our aim is to set out the key principles and code of conduct expected of all members of staff, PTA and volunteers at Thomas Whitehead CE Academy with respect to social networking and to further safeguard and protect children and staff.

Objectives

E-Safety

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

Thomas Whitehead CE Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Social Media

Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image.

In addition, Thomas Whitehead CE Academy has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

Everyone at Thomas Whitehead CE Academy has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

It is important to protect everyone at Thomas Whitehead CE Academy from allegations and misinterpretations which can arise from the use of social networking sites.

Safeguarding children is a key responsibility of all members of staff and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with pupils past or present under 18. The only exception to this is their own children; any pupils who are their children's friends should not be communicated with through social media.

This policy relates to social networking outside work. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorised by the Headteacher.

Roles and Responsibilities

All staff share responsibility for the E-Safety Policy. The school will ensure that IT lessons, assemblies, PSHE lessons, and an age appropriate curriculum for e-safety will support pupils to become safe and responsible users of new technologies. It is the role of the Computing Lead, DSL and Headteacher to;

-  regular monitor any e-safety incident logs
-  regular monitor of filtering / change control logs
-  report to the IT department at The TRUST any concerns

Headteacher and Senior Leadership Team

- + The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Leader.
- + The Headteacher and the DSL should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- + The Headteacher / Senior Leaders are responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- + The Headteacher keeps the e-safety incident logs and ensures that staff are trained on how to report incidents.
- + The Senior Leadership Team will receive regular monitoring reports
- + DSL delivers online safety CPD to staff annually

Computing Lead

- + Leads in monitoring the delivery of online safety lessons through 2 Simple Programme
- + Attains pupil voice

IT Manager Partner

- + that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- + that the school meets required E-safety technical requirements
- + that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- + that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- + that the use of the network / internet / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher DSL
- + that monitoring software / systems are implemented and updated as agreed in school policies
- + Ensure guidelines from KCSIE on Monitoring and Filtering are adhered to

Staff, Parents and Pupils

- + they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- + they have read, understood and signed the Home School Agreement & Pupil Acceptable Use Agreement (KS2) or Home School Agreement & Pupil Acceptable Use Agreement (Foundation / KS1)
- + they report any suspected misuse or problem to the Headteacher or a Senior Leader
- + all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school email or ClassDojo
- + e-safety issues are embedded in all aspects of the curriculum and other activities
- + pupils understand and follow the e-safety and acceptable use policies
- + pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- + they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices (e.g. the appropriate use of cameras on school trips/projects)
- + in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Child Protection Officer and Deputy DDSL

Both the Designated Child Protection and Deputy Officers at Thomas Whitehead CE Academy should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- + sharing of personal data
- + access to illegal / inappropriate materials
- + inappropriate online contact with adults / strangers
- + potential or actual incidents of grooming or cyber-bullying

NB. These are child protection issues, not technical issues, it is simply that the technology provides additional means for child protection issues to develop.

Pupils

All pupils at Thomas Whitehead CE Academy are responsible for using the school digital technology systems in accordance with the Home School Agreement & Pupil Acceptable Use Agreement (KS2 or Home School Agreement & Pupil Acceptable Use Agreement (Foundation / KS1)

- ✚ have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ✚ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- ✚ will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- ✚ should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and the school website.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- ✚ digital and video images taken at school events
- ✚ Social Media websites, in particular, ensuring that no images of children taken on the school premises or whilst on school trips or events are uploaded onto any social media sites (including Facebook and YouTube)

Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach and this forms an essential part of the school's E-Safety and Social Media Policy. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities that enhance childrens' awareness and understanding. At Thomas Whitehead CE Academy we use Purple Mash to deliver a progressive curriculum based on the Education for a Connected World Framework (DFE Feb 2018) Alongside our curriculum we use JIGSAW – A mindful approach to deliver in class lessons, assemblies and to ensure we have up to date information and guidance.

Social Media and Mobile Phones - Protecting Professional Identity

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children, and public in general those with whom they work with. Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

The guidance contained in this policy is an attempt to identify what behaviours are expected of schools' staff who work with children. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential to the designated safeguarding lead.

Code of Conduct: Social Networking

Under no circumstances should staff make reference to any staff member, pupil, parent or school activity/event.

The following are also not considered acceptable:

-  The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
-  The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
-  The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
-  The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.
-  The acceptance of friend requests from pupils past or present under 18 years of age. It is also unwise to accept friend requests from parents or carers of pupils past or present.
-  Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs or videos.

In addition to the above everyone must ensure that they:

- + Communicate with children and parents in an open and transparent way using the school phone number and email address.
- + Never 'friend' a pupil at the school past or present and under 18 years of age.
- + Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- + Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings.
- + Are aware of the potential of online identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct In instances where there has been a breach of the above Code of Conduct, the following will apply:

Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so; because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the Head Teacher.

Filter content lists are regularly updated and internet use is logged and monitored weekly. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering

DIOCESE OF

ST ALBANS

MULTI-ACADEMY TRUST

Believing and achieving together

system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the IT Manager.

Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager and Headteacher.

Publishing on the internet

The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- + The point of contact on the school website should be the school address, school email and telephone number. Staff or pupils' home information will NOT be published.
- + Photographs used on the website of staff will only specify full name and job position and no other personal information
- + Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- + Parents are invited to notify the school if they do not wish their child's photograph to be published on the school website. Parents will be notified of their right to refuse to allow any pictures of their child to be shown. Parents are notified of this right when their child starts school.

Mobile Phones / Cameras / Video Recorder Usage

To ensure the safety and welfare of children in our care personal mobile phones, cameras and video recorders must not be used when children are present.

- + Personal mobile phones should only be used on the school premises when in non-contact time with children and only used during work time in exceptional circumstances, which have been discussed and agreed with a member of the leadership team.
- + Photographs or images of any children within our care may only be taken following parental consent and only using one of the school cameras / iPads. These images should remain within this setting or be shared only with the parents of the child concerned.
- + Personal mobiles, cameras or video recorders cannot be used to record classroom activities. ONLY school property can be used for this.
- + School photographs and recordings can only be transferred to and stored on a school computer.

- ✚ All personal mobile phones must be kept in a secure place (not in a pocket), switched off and not be accessed throughout contact time with the children.
- ✚ In exceptional circumstances, which have been discussed and agreed with a member of the leadership team, staff may keep their phone switched on and accessible as long as they use their phone out of view of children, i.e. in a room designated for staff, e.g. the staff room or an office.
- ✚ During school visits mobile phones should be used away from the children and for emergency purposes only.
- ✚ During a school visit all staff members will follow protocol in the event of an emergency or incident that changes the course of the planned visit such as; injury or traffic. The School Office Manager will be notified directly and will correspond with parents directly. Staff members and parent helpers are not to post anything on social media relating in any way to the emergency.

Data Protection

- ✚ Protection of Personal Information Staff should not give their personal e-mail addresses to children or parents. Where there is a need for communication to be sent electronically the school e-mail address should be used. Likewise staff should keep their personal phone numbers private and not use their own mobile phones to contact children or parents in a professional capacity.
- ✚ There will be occasions when there are social contacts between children and staff, where for example the parent and teacher are part of the same social circle or staff are transport escorts.
- ✚ These contacts however, will be easily recognised and openly acknowledged. Staff have a responsibility to make any such contact known to the senior leadership team.
- ✚ Staff should never share their work log-ins or passwords with other people.
- ✚ Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.
- ✚ Full details can be found in the school's Data Protection Policy. A copy is available on the school website or from the school office.

Cyberbullying

Thomas Whitehead CE Academy define cyberbullying as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual and/or to attempt to gain power and control over them.'

- ✚ In order to reduce the potential for cyberbullying children are not allowed to bring phones to school. Only Y5 and Y6 children who walk to school alone are permitted to bring mobile phones to school once parents have completed a 'Mobile Phone Parental Consent Form'
- ✚ In this circumstance, mobile phones will be switched off, handed to the office and locked away during the school day.

- ✚ Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying.
- ✚ All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance and the 'Mobile Phone Policy' should reduce the risk of personal information falling into the wrong hands.
- ✚ If cyberbullying does take place, employees should keep records of the abuse, text, emails, website or instant message and should not delete texts or e-mails.
- ✚ Staff are encouraged to report all incidents of cyberbullying to their line manager or the Headteacher. Permission to take screen prints of messages or web pages should be sought and a careful log of the time, date and place of the site should be created.
- ✚ All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.
- ✚ All incidents of cyberbullying will be logged and addressed on the advice of the Deputy headteacher for Safeguarding and Behaviour or in her absence a DDSL.

Communications

When using communication technologies the school considers the following as good practice:

- ✚ The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- ✚ The Class Dojo system is a safe and secure system for teachers to communicate directly with parents. Any whole school and class posts will be monitored by Computer Lead.
- ✚ Users must immediately report, to the designated safeguarding lead – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- ✚ Any digital communication between staff and students / pupils or parents / carers (email, chat, etc) must be professional in tone and content. Communications between staff and parents/carers/pupils may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- ✚ Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- ✚ Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Complaints

-  Responsibility for handling incidents will be given to the Headteacher or delegated as the need arises.
-  Any complaint about staff misuse must be referred to the Headteacher or Governors following the school's Complaint Policy.
-  Any illegal apparent or actual misuse will be reported to the Headteacher or the police, as appropriate.

PUPIL ACCEPTABLE USE POLICY AGREEMENT KS2

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep any username and password that I am given safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I
- I will be aware of "stranger danger", when I am communicating online. I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.) If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings. I will not use social media sites.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyberbullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

-  I use the school systems and devices (both in and out of school)
-  I use my own equipment out of the school in a way that is related to me being a member of this school, e.g. communicating with other members of the school.

Name of Student / Pupil: Class:.....

Signed:..... Date:.....

Foundation/ KS1 Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

-  I will ask a teacher or suitable adult if I want to use the computers / tablets
-  I will only use activities that a teacher or suitable adult has told or allowed me to use
-  I will take care of the computer and other equipment
-  I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
-  I will tell a teacher or suitable adult if I see something that upsets me on the screen
-  I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child):.....

Signed (parent/carer):.....

Date:.....