



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

Online Safety Policy

Policy Date: April 2026

Policy Review Date: September 2026

Mission Statement

Trinity is a Christian school with a caring environment in which each individual is valued as special and is encouraged to reach their full potential while enjoying life in all its fullness.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

List of Appendices

Appendix 1	Trinity ICT Acceptable Use Policy (AUP) – Staff and Governors
Appendix 2	Trinity ICT Acceptable Use Policy (AUP) – Supply Teachers, Visitors/Guests
Appendix 3	Trinity Online Safety Rules and AUP (EYFS/KS1)
Appendix 4	Trinity Online Safety Rules and AUP (KS2)
Appendix 5	Trinity Incident Log
Appendix 6	Responding to Online Safety Incident/Escalation procedures

This document will be used in conjunction with the Trinity Behaviour Policy, Trinity Anti-Bullying Policy, Trinity Artificial Intelligence Policy and the Trinity Safeguarding Policy.

1. Introduction

Our Online Safety Policy should be read in conjunction with other related school policies and documents, including Trinity Safeguarding Policy, Trinity Behaviour Policy, Trinity Computing Policy and the Trinity PSHE Policy.

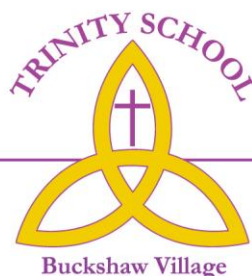
Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

Policies and documents to consider	How is Online Safety included?
School Self Evaluation Framework	Online safety features are part of the safeguarding elements of the School Improvement Plan. Online safety has been highlighted in the ICT area of the school development plan.
Staff Code of Conduct, Recruitment and Induction Procedures	All staff have signed an Acceptable Use Policy regarding the use of ICT in school.
Anti Bullying Policy	Online Bullying is part of the anti-bullying policy.
Behaviour Policy	The acceptable use of technology is included in our Behaviour Policy. There are clear guidelines for dealing with Online Safety issues.
Child Protection Policy	The Child Protection Policy includes references to digital media.
Records Management Policy	How personal data is stored in accordance with the GDPR May 2018.
Privacy Notices – How we use Employee and Children’s Information	How personal data is stored in accordance with the GDPR May 2018.
Remote Learning Policy	Clear guidelines on the use of Online platforms used for remote learning, for pupils working at home (Covid-19)
Artificial Intelligence Policy	Online safety is linked to procedures in place when using AI and educating pupils about AI technologies.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

2. Trinity school's vision for Online Safety

Trinity School provides a diverse, balanced and relevant approach to the use of technology.

- Through a variety of media, the children are encouraged to maximise the benefits and opportunities that technology has to offer.
- The school aims to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
- The children are increasingly being equipped with the skills and knowledge to use technology appropriately and responsibly.
- The school aims to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.
- The users in the school community understand why there is a need for an Online Safety Policy.

3. The role of the Senior Leadership Team.

The role of the Senior Leadership Team and Online Safety co-ordinator include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head Teacher, SLT, staff, pupils and Governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and Practices

This section of the Online Safety Policy sets out the school's approach to Online Safety along with the various procedures to be followed, in the event of an incident.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

4.1 Security and data management

In line with the requirements of the General Data Protection Regulation (GDPR, 2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection
- All devices and removable devices are password protected
- All children have their own password and are encouraged not to share it.

All data in the school is kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy (AUP).

- The Headteacher and Senior Leadership Team are responsible for managing information.
- Staff are aware of where data is located.
- All staff with access to personal data understand their responsibilities.
- The school ensures that data is appropriately managed both within and outside the school environment .
- The staff are aware that they should only use approved means to access, store and dispose of confidential data.
- Staff have access to school logins, to ensure the data remains secure.
- The school's policy on using mobile devices and removable media is that school information is only to be carried on school purchased and password protected and encrypted flash drives, and that all devices which leave school premises are password protected. Staff are not able to access school servers through remote access.
- The school aims to ensure that data loss is managed by the use of passwords for the required people.
- The school's procedure for backing up data is through the service package provided by LCC (Lancashire County Council). It is backed up daily off site.

4.2 Use of mobile devices

The use of mobile devices offers a range of opportunities to extend children's learning. Staff are aware that some mobile devices e.g. mobile phones, game consoles or laptops can access unfiltered internet content.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- Mobile phones are not encouraged to be brought into school by children. If a phone is brought in e.g. needed before or after school, the children must hand the phone in to a teacher or are taken to the office. For children in Years 5 and 6, phones are to be switched off on entry to school premises, collected on entry to the classroom, stored securely during the school day and redistributed at home time/after their afterschool club has finished.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges, particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, social media, assessment or display.

- At school, photographs and video of pupils and staff are regarded as personal data in terms of the GDPR regulations 2018, and the school has written permission for their use from the individual and/or their parents or carers.
- The school seeks consent from the parent/carer or member of staff who appears in the media or whose name is used.
- The parental/carer permission is obtained when pupils enter in Reception but the parents have a right to change this if deemed necessary and are given yearly opportunities to do so, when personal information is updated by the office.
- The staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs of their own children at agreed, specific points, but not during acts of Worship including Christmas and Easter services. They are regularly reminded not to share or post pictures of any other children on Social Media.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- The school ensures that photographs/videos are only taken using school equipment/devices and only for school purposes.
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff must not store digital content on any personal equipment/devices. The staff must not use their own cameras/mobile devices to take photos and have agreed this via the AUP.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy, are monitored by the S.L.T and Governors on an annual basis.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

- All users have access to the Office365 service as the preferred school email system.
- Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved.
- The Netsweeper filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to Lancashire County Council.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The GDPR (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).

Trinity school email disclaimer:

.....
The contents of all e-mail and any attachments are strictly private and confidential and may contain information which is subject to legal privilege. Such e-mail may not be used or disclosed under any circumstances by anyone who is not a named recipient. Please return the e-mail if you are not the intended or named recipient. Unauthorised use of the email or its contents is prohibited and may be unlawful. Incoming and outgoing e-mail is subject to continuous and ad hoc filtering, scrutiny and reporting. The school accepts no liability whatsoever for any damage, loss or expense arising from this e-mail and/or from the accessing of any files attached to this e-mail. This e-mail may not necessarily reflect the views or intentions of Trinity CE Methodist Primary School or its governing body, who therefore do not accept any liability whatsoever for any claims, loss or damages of whatsoever nature, arising directly or indirectly, as a result of the reliance on such information by anyone.

*The addressee's address will not be disclosed to others for commercial intent.
Please notify the school should you not wish to receive e-mail from the school.*

This email has been checked for known viruses.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, X, Whatsapp, Instagram and Snapchat. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.

All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with any pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum security levels. This is regularly checked by the Online Safety Leader.
- Pupils, ex-pupils and parents must not be added as 'friends' on any Social Networking site.
- Children who are under 13 are not legally allowed to be members of Facebook and other such Social Networking Sites.

Remember; whatever means of communication you use, you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile telephones

- The school allows personal mobile phones and smartwatches to be used in school by staff but they are to be left on silent in curriculum time, out of sight of pupils (in classroom store cupboards/staffroom) and are only to be accessed by staff during their allocated break times, unless permission has been given by the Head teacher or Deputy Head teacher in exceptional circumstances – for example, if a member of staff is awaiting an important phone call, e.g. from their Doctor's surgery or child's school. (*Code of Conduct Policy*).
- Call, photo and messaging functions on staff smartwatches should be disabled by staff on entry to the building.
- Staff must not use their mobile phones in corridors or other areas of the school building when children are present.
- The school has a mobile phone which is to be taken on Educational visits and used to contact school/parents as required. It is acceptable for staff to take/use personal mobile phones for school activities e.g. school trips, as long as they are not used to take photographs of pupils and are used when pupils are not present (unless needed in an emergency). (*Code of Conduct Policy*)
- Children in Year 5 and 6, who have permission to walk to and from school and bring a mobile phone to school for safety purposes, e.g. if they walk to and from school alone, must switch their phones off as they enter through the gate or through the main entrance/office. They must then hand in their phones to their teacher when they arrive in class. These will be kept securely in a secure store cupboard, for the duration of the school



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

day and redistributed to pupils at their exit door at the end of the school day. If pupils are attending an after school activity, they must hand their phone to the member of staff registering the club and it will be returned to them at the end of the session. Pupils are not to switch their phones back on until they are exiting through the school gates.

- Pupils who attend School's Out Breakfast Club will turn off their phone on entry to School's Out and hand their phone to a member of School's Out staff, who will store these securely in a secure store cupboard. Children will be given their phones out at the end of the session – these must remain switched off. They will then hand their phone to their teachers to store once they arrive in class at the start of the day.
- Pupils who attend School's Out at the end of the school day, will be given their phone by their teacher when they leave class and it will remain switched off. They will then on entry to School's Out, hand their phone to a member of School's Out staff, who will store these securely in a secure store cupboard. Children will be given their phones back at the end of the session when they are collected by a parent.
- Children must hand their smartwatches into their teacher at the start of the day and these will be stored securely in a secure store cupboard, for the duration of the school day and redistributed to pupils at their exit door, at the end of the school day.
- If a child is found to be using their phone or smartwatch in school, parents will be contacted and staff will follow the behaviour and safeguarding policies to report this.
- Parents are responsible for the safety and security of their child's devices. The school accepts no responsibility for replacing lost / damaged or stolen mobile phones or smartwatches.
- The school accepts no responsibility for students who lose or have their mobile phones or smartwatches stolen whilst travelling to and from school.
- Visitors to school premises are not to use mobile phones or smartwatches at any time. This includes parents at school events in school. Reminders will be given to parents at the start of school events. Parents or visitors may use the office telephone to make calls if necessary. Visual signs on entry doors indicate personal device use is not permitted.
- Special Circumstances e.g. Medical Needs: Students who need to use a smartwatch or mobile phone for medical reasons (e.g. health monitoring, emergency alerts) their parents may request special permission from the headteacher.

Remote Learning Platforms

School has chosen to use the school website, school app and Seesaw for Remote Learning:

- All children in EYFS – Year 6 will be given access to Seesaw and Teaching Staff also have access to all accounts via an admin account.
- Passwords are issued to the children and they are encouraged not to share their passwords. Teachers may need to change passwords to make this more accessible, especially for younger pupils or those with SEND.
- Pupils are taught to use these communication tools in a responsible way in conjunction with the Online Safety curriculum.
- Teachers know how to monitor the use of Seesaw with their class and are given necessary training.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- Accounts are deleted when staff and pupils leave the school. This is monitored by the SLT.
- Please refer to the Remote Learning Policy for further details on the use of Seesaw.

Web sites and other online publications

This may include for example; podcasts, videos, News Reports, vlogs and blogs.

- The school website is effective in communicating Online Safety messages to parents/carers, via the School app/website.
- Everybody in the school is made aware of the guidance for the use of digital media on the website.
- Everybody in the school is made aware of the guidance regarding personal information on the website.
- Teachers have password protected access to edit the school website.
- The Head teacher has overall responsibility for what appears on the website.

Others

The School will adapt/update the Online Safety policy in light of emerging new technologies and any issues or risks associated with these technologies.

4.5 Acceptable Use Policy (AUP)

Our Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs are used for Staff and pupils, must be signed upon entry to school and adhered to by users before access to technology is allowed. This agreement is a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology or have images/videos taken of them, is kept in school and made available to all staff.

Our school AUPs aim to:

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the Online Safety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
 - ✓ Online Bullying
 - ✓ Inappropriate use of email, communication technologies and Social Network sites and any online content
 - ✓ Acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of Online Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

4.6 Dealing with incidents

At Trinity when an incident occurs, the response to this will be determined by the Incident Flowchart (see Appendix 6) and an incident log (see appendix 5) is completed to record and monitor offences. This is audited on a regular basis by the Online Safety Leader or other designated member of the Senior Leadership Team. Any serious issues are escalated to the DSL and are dealt with in line with Safeguarding Policies and Procedures and the school Behaviour Policy. These records are then stored securely on the school server.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation (<http://www.iwf.org.uk>). They are licensed to investigate – schools are not! (See Appendix 11).

Examples of illegal offences are:

- Accessing child sexual abuse images.
- Accessing non-photographic child sexual abuse images.
- Accessing criminally obscene adult content.
- Creating obscene content, e.g. upskirting.
- Incitement to racial hatred/extremism/radicalisation.

More details regarding these categories can be found on the IWF website <http://www.iwf.org.uk>

Inappropriate use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions:

Incident	Procedure and Sanctions
----------	-------------------------



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

Accidental access to inappropriate materials.	<p>Minimise the webpage/ Turn the monitor off/lock device.</p> <ul style="list-style-type: none"> • Pupils to tell a trusted adult immediately. • Enter the details in the Incident Log and report to IT Technician to block using Filtering tool if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	<ul style="list-style-type: none"> • Inform SLT or designated Online Safety coordinator. • Enter the details in the Incident Log. • Additional awareness raising of Online Safety issues and the AUP with individual • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

- The SLT is responsible for dealing with Online Safety incidents. All staff are aware of the different types of Online Safety incidents and how to respond appropriately. e.g. illegal or inappropriate.
- Procedures are in place to deal with Online Safety incidents and all staff aware of these.
- Children are informed of the procedures through discussions with members of staff.
- These incidents are logged in the Online Safety file, on the secure server.
- Incidents are monitored, by the SLT on a regular basis.
- The measures that are in place to respond to and prevent recurrence of an incident.
- The SLT will decide at which point parents or external agencies are involved.
- The procedures are in place to protect staff and escalate a suspected incident/allegation involving a staff member (Appendix 5)

The school uses the 'Online Safety Incident/ Escalation Procedures' document (See Appendix 5) as a framework for responding to incidents.

5. Infrastructure and Technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection systems are in place and are monitored regularly by the IT Technician and Online Safeguarding Co-ordinator.

Pupil access



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

All children are supervised by staff when accessing school equipment and online materials. Clear instructions are given by staff to pupils about which apps and programmes should be used whilst online.

Passwords

- All users of the school network have a secure username and password.
- The administrator password for the school network available to the Headteacher and other nominated senior leader is kept in a secure place.
- Staff and pupils are reminded of the importance of keeping passwords secure
- Passwords will only be changed if the need arises.

Software/hardware

- The school has legal ownership of all software
- The school has an up to date purchase record of appropriate licences for all software and the ICT Technician is responsible for maintaining this.

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The SLT is responsible for managing the security of the school network.
- The safety and security of the school network is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g. computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software on devices.
- Users report any suspicion or evidence of a breach of security to the SLT.
- The school ensures staff to only use School allocated removable storage devices on school equipment e.g. encrypted pen drives.
- The school encourages teachers to follow Online Safety policy guidelines when using their work laptop for personal/family use.
- Web filtering is closely monitored ensuring any inappropriate content is unable to be accessed by pupils, including sites with adult or extremist themes.
- If network monitoring takes place, it is in accordance with the GDPR (2018)
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias
- All internal/external technical support providers are aware of your schools' requirements /standards regarding Online Safety.
- The SLT is responsible for liaising with/managing the technical support staff.

6. Education and Training

In 21st Century society, pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

Our approach to online safety is based on addressing the following categories of risk:

Area of Risk	Examples of Risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites. <i>(including AI systems)</i>	risks such as online gambling, inappropriate advertising, phishing and/or financial scams
Content: Pupils need to be taught that not all content is appropriate or from a reliable source. <i>(including AI systems)</i>	being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies. <i>(including AI systems)</i>	being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
Conduct Pupils need to be taught how to use digital technologies appropriately and respectfully <i>(including AI systems)</i>	personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying;

6.1 Online Safety across the curriculum



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

It is vital that pupils are taught how to take a responsible approach to their own Online Safety. Trinity provides suitable Online Safety education to all pupils with particular reference to:

- Regular, planned Online Safety teaching within a range of curriculum areas, such as Computing and PSHE.
- Online Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Online Bullying and how to seek help if they are affected by these issues, e.g. using peer mentoring. Any Online behaviour issues are dealt with in line with the school Behaviour Policy.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, Online Safety rules (See Appendices), acceptance of site policies when logging onto the school network.
- Pupils are made aware of how the internet can be used to encourage children to participate in illegal activities and how extremist views can be promoted by individuals and/or groups.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- Learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services.

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

6.2 Online Safety – Raising staff awareness

- There is a yearly programme of formal Online Safety training for all staff to ensure they are regularly updated on their responsibilities as outlined in our school policy.
- The Online Safeguarding Leader provides advice/guidance or training to individuals as and when required.
- The Online Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed in staff/team meetings.

6.3 Online Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

The school offers opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies.

For example, through:

- School newsletters, School app messaging, Website and other publications.
- Promotion of external Online Safety resources/online materials.
- Parent Online Safety Workshops, in partnership with different charities and external bodies.

6.4 Online Safety – Raising Governors' awareness



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

The school considers how Governors, particularly those with specific responsibilities for Online Safety, ICT or child protection, are kept up to date. This is through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

NB. The Online Safety Policy will be reviewed yearly (and/or if a serious breach occurs) by the Online Safeguarding Leader, approved by the governing body and made available on the school's website.

6.5 The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks. We have created a separate AI Policy which is to be used in conjunction with the Online Safety Policy.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- *The school will support parents and carers in their understanding of the use of AI in the school (this could be through an "AI in our school guide")*
- *AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI*
- *Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.*
- *We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.*
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

7. Standards and Inspection

At Trinity:

- Online Safety incidents are monitored, recorded and reviewed carefully.
- The SLT are responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is always thoroughly risk assessed.
- These assessments are included in the Online Safety Policy.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.
- These patterns would be addressed most effectively by e.g. working with a specific group, class assemblies, reminders for parents.

List of Appendices

Appendix 1	Trinity ICT Acceptable Use Policy (AUP) – Staff and Governors
Appendix 2	Trinity ICT Acceptable Use Policy (AUP) – Supply Teachers, Visitors/Guests
Appendix 3	Trinity ICT Acceptable Use Policy – Pupils and Parents
Appendix 4	Trinity Online Safety Rules and AUP (EYFS/KS1)
Appendix 5	Trinity Online Safety Rules and AUP (KS2)
Appendix 6	Trinity Incident Log
	Responding to Online Safety Incident/Escalation procedures



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

Appendix 1

Trinity - ICT Acceptable Use Policy (AUP)

Staff and Governor Agreement

ICT and the related technologies such as email, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with pupils and other adults are appropriate.
8. I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes.)
9. I will not install any hardware or software without the prior permission of the SLT.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will report any known misuses of technology, including the unacceptable behaviours of others.
13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
15. I have a duty to protect passwords and personal network logins and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
16. I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
19. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
20. I will take due care of any portable ICT equipment given to me to use for school purposes, and accept that if items (e.g. laptops, tablet computers) are taken offsite, that they are not insured for loss or damage caused by theft or accident. I understand that I will remain solely responsible for their replacement, should theft / an accident /damage to equipment occur offsite.
21. I agree that I will ensure that any portable storage devices, such as USB sticks are checked by the IT Technician before use to ensure that they do not contain viruses or any data which may corrupt the equipment in school.
22. I agree that personal mobile phones will not be used anywhere in or out of school (at offsite school events) when pupils are present and that no images/videos of pupils will be taken using a personal mobile device. This is in agreement with the staff Code of Conduct.
23. When using AI systems in my professional role I will use these responsibly and:
 - will only use AI technologies approved by the school
 - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
 - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
 - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
 - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature Date

Full Name(PRINT)

Position/Role

Appendix 2

Trinity - ICT Acceptable Use Policy (AUP)

Supply teachers and Visitors/Guests Agreement

For use with any adult working in the school, for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will respect copyright and intellectual property rights.
4. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
5. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
6. I agree that I will not use a personal mobile device to make phone calls or take any images/video on site. If I need to make a telephone call I will use the main office phone, or use a personal mobile device offsite.
7. I will not install any hardware or software onto any school system.
8. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
9. I agree that I will ensure that any portable storage devices, such as USB sticks are checked by the IT Technician before use to ensure that they do not contain viruses or any data which may corrupt the equipment in school.
10. When using AI systems in my professional role I will use these responsibly and:
 - will only use AI technologies approved by the school
 - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

head@trinitybuckshaw.lancs.sch.uk

- to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature Date

Full Name (PRINT)

Position/Role

Appendix 3 & 4

Online Safety - Pupil and Parent Acceptable Use Policy (AUP)

As part of the National Curriculum, all pupils use technology including the internet and information technology devices in their learning. Both pupils and their parents/carers are asked to sign below to show that the Online Safety Rules have been understood and agreed.

Name of Pupil:	Class:
----------------	--------

Pupil Agreement

- *I have read and I understand the school Online Safety Rules.*
- *I will use computing devices, the school network, the internet and other new technologies respectfully, carefully and sensibly at all times.*
- *I know that the network, apps and internet pages that I access might be checked by an adult.*

Signed:	Date:
---------	-------

Images

To help your child learn, children may be photographed and these images used for assessment, to record learning or help present their ideas. Please tick below:

I agree that my child may have their photograph taken for learning purposes.	Yes		No	
I agree that my child may be videoed for learning purposes.	Yes		No	
I agree for images or videos of my child to be used on the school website / in the School prospectus.	Yes		No	



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

head@trinitybuckshaw.lancs.sch.uk

I agree for images or videos of my child to be used on School Social media posts e.g. on Instagram/Facebook.	Yes		No	
I agree for images or videos of my child to be used on Seesaw for learning purposes.	Yes		No	
I agree that images and video of my child may be used in other external media, such as local newspapers /TV and their online websites/Social Media.	Yes		No	
Internet I understand that the school will take every reasonable precaution, including filtering systems, to ensure that children will feel safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and when using mobile technologies.				
I grant permission for my child to use the Internet for Independent work.	Yes		No	
Signed (Parent/Carer):	Date:			

Appendix 3 Online Safety Rules (EYFS/KS1)



To **#BESAFE**
when using digital
devices and the
Internet we will...



Be polite
and friendly
when using
online tools.

Explore the
Internet safely,
when an adult
is with us.



Secret.



Never give out
personal information

Ask an
adult if
we need
help using





Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

head@trinitybuckshaw.lancs.sch.uk

Appendix 4 Online Safety Rules (KS2)



To #BESAFE
when using digital
devices and the
Internet we will...



Be polite and friendly when communicating using online tools and digital devices.

Explore the Internet safely, with the permission of an adult and when an adult is present.



Secret.



Never give out our own or others' personal information and passwords; be careful

Approved.

Only use Apps, programs and digital content





Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk

Appendix 5 – Online Safety Incident Log

All Online Safety incidents must be recorded by the School Online Safety coordinator and SLT. . This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving Online Bullying should also be recorded on the 'Integrated Bullying and Racist Incident Record Form 2' available via the Lancashire Schools' Portal.

Name of person reporting incident:			Position:				
Date of incident:							
Where did the incident take place?							
Description of the incident							
Name(s) of those involved:							
Age(s) / Year group of child(ren) involved:							
How was the content accessed?							
School internet via a PC/laptop		via an app		via a school tablet		via email	



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

head@trinitybuckshaw.lancs.sch.uk

Tablet using alternative provider		via a mobile phone using an alternative provider		via a social media website		
Other (give details)	Appendix 6 – Responding to Online Safety Incident/ Escalation Procedures					
What action will be taken	Taken from SWGfL Online Safety Policy Template					

Designated Safeguarding Lead (DSL) notified of an Online Safety incident¹

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required

Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA, LADO and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.
Remember, do NOT investigate yourself.

Await Police response

Police response received



Trinity Church of England/Methodist Primary School

— BUCKSHAW VILLAGE —

Headteacher: Mrs Jill R Wright

✉ head@trinitybuckshaw.lancs.sch.uk