



Trinity St Mary's Church of England Primary
School

ICT Acceptable Use and E-Safety Policy Summer Term 2023

"Many Hearts Make A School"



1. Aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses pose risks to data protection, online safety and safeguarding. Our school aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for schools
- Protecting Children from Radicalisation
- Equality Act 2010

The policy also takes into account the [National Curriculum computing programmes of study](#).

3. Definitions

- **ICT Facilities:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **Users:** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Roles and responsibilities

4.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

4.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

4.4 The ICT Technician

The ICT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- "The 2John's" <https://esafetytraining.org/>
- National Online Safety (we are a certified school) <https://nationalonlinesafety.com/>

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website where it is felt appropriate. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying, when it is felt appropriate, to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Unacceptable use

The following is considered unacceptable use of the schools ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behavior proceedings (see section 4.2 below).

Unacceptable use of the schools ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, application or web services on the school's network without approval by the authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

7.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

Any individual seeking to use the school ICT facilities for a purpose that would normally be considered an unacceptable use should put in writing to the Headteacher their requirement and reason.

7.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behavior and discipline. Copies of the school's behaviour and disciplinary policies can be obtained from the school office.

8. Staff (including governors, volunteers and contractors)

8.1 Access to school ICT facilities and materials

The school's IT Technician manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the School Business Manager.

8.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the School Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

8.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during normal work time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Bring Your Own Device policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

8.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

8.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

The school uses Microsoft Remote Desktop Web Access, this is managed by our external IT contractor.

You will be required to have a school login before you can access the schools ICT remotely. This is provided by the IT Technician along with information on how to use Remote Access. Access has to be approved by either the Headteacher or the SBM.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the external IT Contractor or the IT Technician may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy. A copy of our data protection policy can be found on our website or in the school office.

8.4 School social media accounts

The school has an official Twitter page, managed by the Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

8.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited

- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

9. Pupils

9.1 Access to ICT facilities

Computers and equipment are available to pupils only under the supervision of staff.

9.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

9.3. Pupils using mobile devices in school

Pupils may bring mobile devices into school if they walk to or from school on their own. These mobile devices are left switched off and in the school office for the duration of the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Parents

10.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

10.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

11. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

11.1 Passwords

All staff using the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Pupils passwords are supplied with new passwords at the beginning of the school year by the IT Technician. Pupils are restricted from changing their own passwords and these can only be changed by the IT Technician or the external IT contractor.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

11.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

11.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. A copy of the school's data protection policy can be found on our website or the school office.

11.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the IT Technician.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the School Business Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

11.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT Technician.

12. Internet access

The school wireless internet connection is secured.

The school has 2 WiFi secure logons one for staff and pupils and a second one for guests to the school.

There are 5 different levels of filtering which is controlled by our broadband supplier. The level of filtering is set differently for younger children, older children and staff, to restrict access to certain websites and content.

Filtering is not always going to work and can either let someone onto an inappropriate website or block them from one that is required. If this happens it should be reported to both the IT Technician and the SBM immediately.

12.1 Pupils

Pupils do not have access to wifi except when using school devices.

12.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring and review

The DSL logs behaviour and safeguarding issues related to online safety using the behaviour and safeguarding monitoring system 'CPOMS'.

The headteacher, School Business Manager and IT Technician monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

15. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning

This policy was agreed by the governing body in the summer term 2022.

Signed on behalf of the governing body:

Date:

It will be reviewed in Summer Term 2025.

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'.

Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if...

A pupil adds you on social media

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to Facebook or the relevant social network and ask them to remove it

If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carers:	
Name of child:	
<p>Online channels are an important way for parents/carers to communicate with, or about, our school.</p> <p>The school uses the following channels:</p> <ul style="list-style-type: none">Our official Twitter pageEmail/text groups for parents (for school announcements and information)Our website <p>Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).</p>	
<p>When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:</p> <ul style="list-style-type: none">Be respectful towards members of staff, and the school, at all timesBe respectful of other parents/carers and childrenDirect any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure <p>I will not:</p> <ul style="list-style-type: none">Use private groups, the school's Twitter page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate wayUse private groups, the school's Twitter page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incidentUpload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	Date:

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them for non-educational purposes
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean, rude or inappropriate language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people
- Give my personal information (including my name and contact details) to anyone without the permission of my teacher or parent/carers
- Arrange to meet anyone offline without first consulting my parent/carers, or without adult supervision

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

I will only bring a mobile phone onto the school premises if I have the permission of my parent/carers to leave the school site at the end of the day without an adult. I will leave my phone switched off in the office and I will not turn it back on until I have left the school site.

Signed (pupil):

Date:

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT Technician know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	