Online Safety, ICT and Internet Acceptable Use Policy

St Thomas More Catholic Academy

Role	Name	Contact Details
Designated Safeguarding Lead	Mrs. J. Stubbs	01782 882900
Deputy Designated Safeguarding Leads	Mrs. A. Staton/Mrs K Williams	01782 882900
Early Help Champion	Mrs. A Staton	01782 882900
Nominated Academy Representative	Mrs. C. Goodwin	office@stmca.org.uk
Headteacher	Mr. M. Rayner	01782 882900
Online Safety Lead	Mrs. J Stubbs	01782 882900
Local Authority Designated Officer (LADO)	John Hanlon	01782 233342
Safeguarding Referral Team (Children's Social Care Stoke-on-Trent)	Mon – Thurs: 8.30am - 5pm Fri:8.30am – 4.30pm	01782 235100
Emergency Duty Team (Children's Social Care Stoke-on-Trent)	Out of hours (above)	01782 234234
Stoke-on-Trent Safeguarding Children Board	www.safeguardingchildren.stoke.gov.uk	
Stoke-on-Trent Safeguarding Children Board Agency Representative	Sangita Mishra sangita.mishra@stoke.gov.uk	01782 235897

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Online safety policy

Approved by:	Mr R Flello: Chair of the Local Academy Representatives	**Date:**	
Last reviewed on:	September 2023		
Next review due by:	September 2025		

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for students, 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 also pose risks to data protection, online safety, cyber security and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, 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, cyber security and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students 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 emerging technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policies

2. Relevant 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 2023 (publishing.service.gov.uk)
- Searching, screening and confiscation: advice for schools
- Filtering and monitoring standards for schools and colleges
- Cyber security standards for schools and colleges
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education

- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
- DfE guidance on protecting children from radicalisation.
- It also reflects existing legislation, including but not limited to Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk), 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.

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, students, 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

3. Roles and responsibilities

3.1 The Local Academy

The Local Academy board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governor who oversees online safety is the Safeguarding link governor.

All governors will:

- Ensure that they have read and understand this policy
- Support the school in encouraging parents/carers and the wider audience to become involved in online safety activities.
- Review annual records and reports of the annual online safety audits.

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's DSL are set out on the front page of this policy.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged via CPOMS and dealt with appropriately in line with the school behaviour policy
- Supporting the Online Safety Lead in coordinating staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Reporting any significant beaches of the policy

This list is not intended to be exhaustive.

3.4 The Senior Operations Manager

The Senior Operations Manager alongside the Network Manager 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 to ensure infrastructure is secure and not open to misuse or malicious attack meeting 'Cyber security standards for schools and colleges'
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis an half termly basis reporting to the Headteacher
- Blocking access to identified/known potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Monitoring Software/systems are implemented and regularly updated as agreed in school polices in line with 'Filtering and monitoring standards for schools and colleges'
- Provide updates to DSL and Headteacher regarding any technological changes or implications for online safety

This list is not intended to be exhaustive.

3.5 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 within the Staff Code of Conduct and the Safeguarding Policy, and ensuring that pupils follow the school's terms on acceptable use, as stated within the Home School Agreement
- Working with the DSL to ensure that any online safety incidents are logged 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

- Supervising and monitor the use of digital technologies, mobile devices, cameras etc in lessons. The school does not allow the use of personal mobile devices during the school day which all staff are aware of the procedures.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Incidents and concerns should then be recorded on CPOMS

This list is not intended to be exhaustive.

3.6 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 within the Home School Agreement
- Reinforce the online safety messages provided to learners in the school

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody
- UK Council for internet safety
- SWGFL Internet safety for Parents
- Vodafone Digital Parenting Magazine

4. Unacceptable use

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

Unacceptable use of the school's 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
- Not undertake any activities that might be classed as cyber-crime under the Computer Misuse Act (1990)

- 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
- Using a portable device to access media or install software / files on the school system without permission
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, 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, applications or web services on the school's network without approval by 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.

4.1 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.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies

Sanctions could include:

> Revoking permission to use the school's systems

> Detentions

> Fixed term inclusion / suspension

> Permanent exclusion

> Police action

> Response in line with the school's Disciplinary Policy and/or Staff Code of Conduct

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The Network Manager 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 network manager.

5.1.1 Use of phones and email

- The school provides each member of staff with an email address.
- This email account is monitored and its use should mirror the Staff Code of Conduct.
- 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 students, 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, (this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as; how to handle education and safeguarding information) 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 Senior Operations Manager immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or students. 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.

5.2 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 contact time/teaching hours/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students 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 Staff Code of Conduct

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 students 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.

5.2.1 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).

5.3 Remote access

We allow limited staff access to the school's ICT facilities and materials remotely where their role requires access to software restricted to the remote access server.

The school's Network Manager manages remote access.

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

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.

5.4 School social media accounts

The school has an official Facebook, Instagram and Twitter page, managed by the school's Senior Operations Manager. 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.

Any queries for social media should be directed to the Senior Operations Manager.

5.5 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

6. Students

6.1 Access to ICT facilities

Pupils may bring mobile devices into school, but are not permitted to use them during school time.

Computers and equipment in the school's ICT suite are available to students under the supervision of staff

Some students may have unsupervised access e.g. sixth formers and KS4 students at the discretion of the school.

Students do not have access to the school's wifi.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the school's behaviour policy, if a student 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, including against any protected characteristic or any behaviours that could be deemed as hate crimes in the eyes of the law
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity, including extremist views or thoughts
- 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 students, 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
- Compromising the cyber security
- Bringing devices such as USBs to add games, programmes or software to school equipment without prior approval

Please see section 4.2 above .

7. Parents

7.1 Access to ICT facilities and materials

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

7.2 Communicating with or about the school online

We believe it is important to model for students, 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 Home School Agreement, as acknowledgment.

7.3 Parents and visitors Acceptable Use

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 Senior Operations Manager 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.

8. 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, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. All users will be forced to reset their passwords every 6 months.

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 students 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.

8.2 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.

Regular checks are completed on software, firewalls and antivirus software by the Network Manager.

8.3 Data protection / GDPR

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 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 Network Manager.

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 Network 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.

8.5 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 student information) out of school if they have been specifically authorised to do so by the Senior Operations Manager.

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

8.6 Filtering and Monitoring

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system. These will be in line with 'Filtering and monitoring for schools and colleges'.

The Network Manager will ensure the filtering provider is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

- **Filtering systems:** block access to harmful sites and content
- **Monitoring systems:** identify when a user accesses or searches for certain types of harmful content on school and college devices (it doesn't stop someone accessing it). The school / DSL is then alerted to any concerning content allowing them to intervene and respond.

Expectations for staff: Reporting a concern

- The expectations, applicable roles and responsibilities in relation to filtering and monitoring form part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens
- Staff should report a concern when/if:
    - They witness or suspect unsuitable material has been accessed
    - They are able to access unsuitable material
    - They are teaching topics that could create unusual activity on the filtering logs
    - There is failure in the software or abuse of the system
    - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
    - They notice abbreviations or misspellings that allow access to restricted material

8.7. Monitoring arrangements

- The DSL oversees the logging of behaviour and safeguarding issues related to online safety through CPOMS.
- An annual review of the online safety filtering and monitoring systems will be conducted and reported on by the Network Manager to ensure the standards are being met using resources such as 360 safe websites.
- The Network Manager will be responsible for
    - Maintaining filtering and monitoring systems
    - Providing filtering and monitoring reports
    - Completing actions following concerns or checks to systems
- These checks will include

    - School owned devices and services, including those off site
- A log of checks will include
    - When the checks took place
    - Who completed the checks
    - What was checked and tested
    - Any resulting actions
- The Network Manager will ensure that it will identify
    - device name or ID, IP address, and where possible, the individual
    - the time and date of attempted access
    - the search term or content being blocked
- The Network Manager will liaise with the DSL and Senior Operations Manager if there are any concerns over Anti-Phishing and it will be reported to https://apwg.org/

8.8 Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their portable hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Encouraging online storage including One Drive, Sharepoint, Teams and appropriate permissions

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager

8.9 Expectations for staff: Reporting a concern

The expectations, applicable roles and responsibilities in relation to filtering and monitoring form part of their safeguarding training. For example, part of their role may be to monitor what's on students' screens

Staff should report a concern when/if:

- They witness or suspect unsuitable material has been accessed
- They are able to access unsuitable material
- They are teaching topics that could create unusual activity on the filtering logs
- There is failure in the software or abuse of the system
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- They notice abbreviations or misspellings that allow access to restricted material

8.10 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 deputies 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 Safeguarding Policy.

9. Internet access

The school wireless internet connection is secured.

All pupils, parents, staff, volunteers and governors complete an agreement before logging into the school network.

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors by Securus to ensure they comply with the above.

10 Educating Pupils About Online Safety

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

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Year 7	Year 8	Year 9
• Acceptable use policy • Username • Password Log in • Email, Cloud computing • Digital wellbeing	• Digital Footprint • Social Media • Passwords, • Phishing, • Malware, • Shoulder Surfing, • Hyperlink, • Encryption, • Trojans, • Viruses, • Fire wall • Anti-Virus Software, • Privacy Settings	• Responsible users: Two Factor Authentication, • Acceptable Use Policy, • Cloud Computing, • Crediting, • Copyright, • Creative Commons License, • E-Waste, • GDPR, • Data Protection Act

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

Year 7	Year 8	Year 9	Year 10	Year 11
Online Presence Self-Esteem Harmful Sexual Behaviour Public sexual Harassment	Bullying (Cyberbullying) Stereotypes / Prejudice Equality Act 2010 Pornography Harmful Sexual Behaviour Public sexual Harassment	Physical Consent Exploitation Social Media – online scam Harmful Sexual Behaviour Public sexual Harassment	Protected Characteristics, Image sharing Harmful Sexual Behaviour Public sexual Harassment	Respectful Relationships, Image sharing risks, Image sharing Law Digital Footprint Explicit Content, Consent, Grooming Harmful Sexual Behaviour Public sexual Harassment

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

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

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

11. 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 or social media. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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.

12. Cyber bullying

12.1 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 and anti-bullying policy.)

12.2 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. Staff will discuss cyber-bullying with their tutor groups.

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 will also use external agencies to promote positive use of technology including the police.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying 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.

Appendix 1: Facebook Top Tips For Staff

Don't accept friend requests from students 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 students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your students 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 students)

Please be aware that comments which could be deemed to be racist, sexist, of a sexual nature, discriminate against a protected characteristic or constitute a hate crime could result in disciplinary action by the Headteacher.

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students 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 student adds you on social media

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

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

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

Notify the DSL on 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
- Students 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 student 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