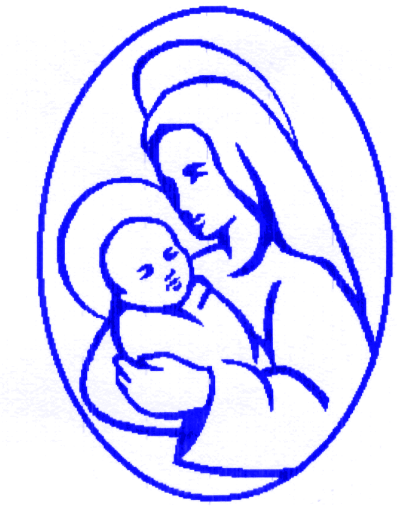
St. Mary's Church of England Primary School, High Crompton



E-Safety & Acceptable Use Policy

Updated and Reviewed : September 2022
Approved by Governors on: 29.9.22
Review Date: December 2025
Signed by chair A Green

SCHOOL VISION

'Love one another as Jesus loved us.' (John 13 v 34-35)

Jesus said, 'Love one another as I have loved you'.
Through God's love and our Christian Values, we encourage each individual to love, respect and value themselves and others.
We encourage and nurture the growth of every individual and their uniqueness so that all flourish and become all that they can be and all that God made them to be.

HEALTHY SCHOOL

St. Mary's is a Healthy School with healthy attitudes embedded in the curriculum and extra-curricular activities. Pupils are encouraged to be active and maintain healthy relationships with their peers and adults as well as making choices about healthy lifestyles.

BUILDING LEARNING POWER STATEMENT

At St. Mary's, we encourage all pupils to build their own learning power. Building Learning Power emphasises the development of lifelong learning values and skills. We aim to ensure that all pupils develop persistence and curiosity for learning and become adventurous risk takers who are not afraid of the 'don't know' state of mind. At St. Mary's, pupils will develop the ability to take responsibility for their own learning and self assess and be able to articulate themselves as a learner. They will have the opportunity to develop the ability to know what's worth learning, know how to face confusion and know the best learning tool for the job.

1.0 Introduction

The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect pupils from potential and known risks

The school has appointed an e–Safety Lead Mrs Ashley Burke. Our e–Safety Policy has been written by the school, building on advice from OLSCB and government guidance including the recent publication 'Teaching online safety in schools' June 2019.

The focus for this policy is to ensure that existing policies (such as those on safeguarding and child protection, , safer working practices, anti-bullying, the curriculum and behaviour) are applied to the digital environment. In order for this to happen these policies are regularly reviewed against the Local Authority's and national guidance, and updated as necessary.

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), 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 and safeguarding.

This policy 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
- The responses necessary when a risk to a child is discovered

Safeguarding pupils, including e-safety is everyone's responsibility. E-safety is therefore not just the responsibility of the e–Safety Coordinator, the Computing Subject Leader, the Headteacher or the IT Technician.
Breaches of this policy may be dealt with under our Behaviour Policy, Safer Working Practices/Staff code of conduct, Safeguarding and Child Protection Policy.

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 2022
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools (2019)

3. 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
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- 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, 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
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher and Governors 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.

3.1 Sanctions

If children break the rules as laid down by this policy, they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy, they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken, the police will be informed, and the school will assist the police with any prosecution

See also Behaviour policy, Safeguarding and Child Protection Policy and Safer Working Practice

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

4.1 Access to school ICT facilities and materials

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

- Computers, tablets, mobile phones 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 Headteacher, Business Manager and/or Fingertip Solutions.

4.1.1 Use of phones and email

The school provides each member of staff and governor 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 and governors must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted/ sent securely 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 that contains the personal information of another person, they must inform the Headteacher 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.

4.2 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 teaching time or directed 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 4.5). 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 Safer Working Practice Policy and Staff Handbook.

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.

4.2.1 Personal social media accounts

Members of staff should ensure 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 7).

4.3 School social media accounts

The school has an official Twitter page, managed by SLT. 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.

4.5 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

5. Pupils

5.1 Teaching and Learning

Whilst recognising the considerable benefits of new technologies, we teach pupils to protect themselves from the 3Cs which underpin all aspects of an approach to e-safety:

- inappropriate **content**
- undesirable **contact**
- hurtful **conduct**

Research indicates that pupils who are given greater freedom at school to use new technologies have a better knowledge and understanding of how to stay safe online. It is therefore important that this school runs a 'managed system' that helps pupils to become safe and responsible users of technology by allowing them to take more responsibility and manage their own risk. We believe that pupils become more vulnerable if they are not given the opportunity to learn how to assess and deal with online risk for themselves.

To support this, the school has adopted the Oldham Charter of Young People's Digital Rights and this is shared widely with pupils in all classes. (See Appendix 2)

Any pupil can be vulnerable online, however staff should be mindful that for some pupils, for example looked after children and those with special educational needs may be more susceptible to online harm. All pupils will have access to an e-safety curriculum.

5.1a Why use on-line technology?

- The Internet is an essential element in the 21st century life for education, business and social interaction.
- The school has a duty to provide students with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- Pupils use the Internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security when online.

5.1b How does on-line technology enhance learning?

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Pupils are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils.

- Access to the internet may be by teacher or teaching assistant demonstration.
- Pupils may access teacher-prepared materials through the shared folder on the school server or school Intranet, rather than the open Internet.
- Pupils may be given a suitable web page or a single website to access.
- Pupils may be provided with lists of relevant and suitable websites.
- Older, more experienced pupils, may be allowed to undertake their own internet search having agreed a search plan with their teacher. Pupils will be expected to observe the rules for acceptable use.
- Pupils accessing the internet will be supervised by an adult at all times.

5.1c Pupils will be taught to evaluate internet content

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that most of the information on the Internet is intended for an adult audience and that much of the information on the Internet is not properly audited/edited. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television.
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium).
- When copying materials from the internet, pupils will be taught to observe copyright.
- Pupils will be made aware that the writer of an e-mail or the author of a webpage may not be the person claimed.

5.1d E-safety education / curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. Staff need an understanding of the risks that exist online so that they can tailor their teaching and support.

Potential harm or risks include:

- age restrictions

- content: how it can be used and shared
- disinformation, misinformation and hoaxes
- fake website and scam emails
- online fraud
- harvesting/farming of online personal data
- persuasive design
- privacy settings
- targeting of online content
- online abuse
- content which incites
- fake profiles
- grooming
- live streaming
- pornography
- unsafe communication
- impact on confidence (including body confidence)
- impact on quality of life, physical and mental health and relationships
- online behaviour versus offline behaviour
- reputational damage
- suicide , self harm and eating disorders

(See 'Teaching online safety in school' June 2019 for further descriptions and information.)

The education of pupils in e-safety is therefore an essential part of the school's computing and RSHE provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience online. They also need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Teaching about online safety is within a whole school approach and should be a focus in all aspects of school life including within policies, curriculum schemes of work, proactively engaging with parents/carers, having clear expectations of how pupils behave online and that staff have appropriate training. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / RHSE / other lessons and should be regularly revisited (see St Mary's schemes of work).
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school. (See appendix 4)
- Staff, Governors and volunteers should act as good role models in their use of digital and online technologies and are required to sign an Acceptable Use Agreement. (See appendix 3)
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.

5.1e Parents / Carers

Some parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their pupils and in the monitoring / regulation of the pupil's on-line behaviours. Parents may under estimate how often pupils come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities

- Letters, newsletters, website, tweets
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

6.0 Managing the use of on-line technology

This sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. The policy details how we provide support and guidance to parents / carers for the safe and responsible use of these technologies by adults and pupils

In order to prevent inappropriate situations occurring it is important that staff, volunteers and pupils are aware of their responsibilities and the expectations whilst using technology. Each user signs a contract to ensure that they know what is deemed 'acceptable use of the internet'. (See appendices 3&4).

6.1 The e-safety Lead

At St. Mary's CE Primary School the e-safety lead works closely with the designated person for Safeguarding. Mrs Ashley Burke is the school's e-safety lead and Mrs Pamela Hartley (Headteacher) is the school's designated person for Safeguarding and Child Protection. The responsibilities of the lead person include:

- Updating the policy
- Ensuring that policies and procedures include aspects of e-safety for example the anti-bullying policy includes cyber-bullying
- Working with the ICT Technician to ensure that filtering is set at the correct level for staff and pupils.
- Ensuring that staff training is provided on e-safety issues
- Ensuring that e-safety is included in staff induction
- Monitoring and evaluating incidents that occur to inform future safeguarding

6.2 Password Security

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

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.

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

For pupils to access the school network there is a general 'log in' for each year group. This gives access to the Internet and a variety of software. All work is saved directly onto the school server. Pupils do have their own log in and passwords for the MyMaths, Spag.com, Times tables Rockstars, IXL and 'Purple Mash' which they are taught to keep secret and not to share with others. Pupils are instructed to inform their teacher if they think their password has been compromised or someone else has become aware of their password.

6.3 Managing Specific on-line Technologies

6.3.1 *Internet Access*

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form for their child to use the Internet

- At Key Stage 1, access to the Internet will be by adult demonstration and direct supervised access to specific, approved on-line materials
- At Key Stage 2, pupils will work independently using the Internet, but will not be left unsupervised.
- Parents will be asked to sign and return a consent form.

6.3.2 *Email*

- Through 'Purple Mash', pupils have their own email accounts and passwords. Emailing is currently restricted to communication within the school.
- Pupils are instructed to tell a teacher if they receive offensive email.
- Pupils cannot send messages to external organisations.

6.3.3 *The school website:*

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully to ensure that no photograph has only one pupil image on it.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website or Twitter.

6.3.4 *Chat and instant messaging*

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not access social networking sites for example 'Facebook' or 'Instagram'.
- Pupils should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- Any form of bullying or harassment is strictly forbidden.

6.3.5 *Filtering*

- The School works in partnership with parents, the LA, Internet Service Provider, Fingertip Solutions technical support and DFE to ensure that systems are in place to protect pupils.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Local Authority (https://www.oldham.gov.uk/lscb) via the e-safety lead.
- Any material that the school believes to be illegal must be referred to the internet Watch Foundation (https://www.iwf.org.uk)

6.3.6 *Photographic, video and audio technology*

- When not in use, video conferencing cameras should be switched off .
- It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. School equipment should be used for this purpose. Should personal equipment ever be used, then all images must be transferred to school hardware and deleted from the personal device as a matter of urgency.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
- Pupils should always seek the permission of their teacher before making audio or video recordings within school grounds.

- This guidance around images applies also to moving images – i.e. video and video links. Care should be taken with the security of video files on computers, servers, and portable drives, as well as those remaining on a video camera after use. Any copies unsecured (e.g. on the video camera itself) should be deleted. Use of technologies such as Skype, Facetime, or 'old-style' video-conferencing should be undertaken within these same guidelines.

6.3.7 *Mobile Phones/Devices*

- Pupils are not allowed mobile phones in school. However it is recognised that for older pupils some parents / carers may wish them to have a mobile phone with them if they walk to/from school on their own. In these circumstances permission must be requested in writing to the Headteacher. In such instances, mobile phones must be switched off whilst on the school grounds and the school takes no responsibility for loss, theft or damage. All phones in this instance should be left safely with their classteacher.
- Staff must have their mobile phones switched off during teaching time.
- The sending of abusive or inappropriate text messages is strictly forbidden.
- Signage instructs all visitors to turn off their mobile phones when coming onto the premises to prevent any images being recorded.
- All professionals working with young people who use personal mobile devices should ensure that they have an appropriate pass code set to prevent access by anyone who has taken the device. Similarly, passwords for email and other online services should not be saved on the device.
- Mobile devices should not be used to store pupil's personal data (and nor should laptops). It is perfectly reasonable and normal for teachers, for example, to have spreadsheets of assessment data, targets, etc that they use for monitoring and analysis but not personal data (such as home addresses, contact telephone numbers, medical information, photographs etc) which should never be needed on such a device.
- Sexting is where young people share sexual images of themselves. Where this happens, images have usually been shared with a partner or intended partner as a form of flirtation or - in the eyes of the young person - 'safe sex'. This act itself poses a risk to the young person in the image: once it has been shared it is liable to be distributed further. This action may also place both the sender and the recipient in a position of having committed an offence under the Protection of Children Act 1978.Young people of an age likely to consider such actions should be educated about the risks.

6.7.8 *Emerging* ICT Applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7.0 Complaints regarding the use of on-line technology and responses necessary when a risk to a child is discovered.

Prompt action is required if a complaint is made. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the School's Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with the school's safeguarding policy.
Any complaints about staff misuse of on-line technology must be referred directly to the Headteacher.

8.0 How to respond when a risk is discovered

The headteacher and e-safety lead will ensure that the following procedures are adhered to in the event of any misuse of the Internet:

8.1 An inappropriate website is accessed inadvertently:

- Report website to the Headteacher and e-safety lead.
- Contact the filtering service so that the site can be added to the banned or restricted list.
- Log the incident. (See appendix 5) and upload to CPoms

8.2 An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the Headteacher and e-Safety lead immediately.
- E-safety lead to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the filtering services as with 8.1 in order to reassess the filters.

8.3 An inappropriate website is accessed deliberately by a child:

- Refer the child to the Acceptable use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can/may be informed.
- Log the incident
- Decide on appropriate sanction.
- Notify the parent / carer.
- Contact the filtering service to notify them of the website.

8.4 An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher and e-Safety lead immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police, social care CEOP.
- Log the incident.

8.5 An illegal website is accessed or illegal material is found on a computer.

8.5.1 The following incidents must be reported directly to the police:

- Indecent images of pupils found. (Images of pupils whether they are photographs or cartoons of pupils or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Criminally racist or anti-religious material
- Violent or bomb-making material
- Extremism and radicalisation material (refer to The Prevent Duty)
- Software piracy
- The promotion of illegal drug-taking
- Adult material that potentially breaches the obscene publications act 1959 in the UK.
- Harassment

If any of these are found, the following should occur:

- Alert the Headteacher and e-Safety lead immediately.
- DO NOT LOG OFF the computer but disconnect from the electricity .
- Contact police and or CEOP/ Channel and social care immediately (Police – 0161 856 8962, social care – 0161 770 3790, pupils over 16 – 0161 770 6599, out of hours – 0161 770 6936).
- If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the school, Safeguarding lead who will then liaise with the Local Authority Designated Officer.

8.6 An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)

- Ensure the child is reassured and remove them from the situation.
- Report to the Designated Person for Safeguarding immediately, who will then follow the Allegations Procedure and Child Protection Procedures www.oldham.gov.uk/lscbhome
- Report to the Local Authority Designated Officer
- Preserve the information received by the child if possible.
- Contact the police as necessary.

8.7 Threatening or malicious comments are posted to the school website or social media (or printed out) about an adult in school:

- Preserve any evidence and log the incident.
- Inform the Headteacher immediately and follow Safeguarding and Child Protection Policy.
- Inform the e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP if appropriate.

8.8 Where staff or adults have posted on inappropriate websites, or have inappropriate information about them posted:

- This should be reported to the Headteacher follow Safeguarding and Child Protection Policy and Safer Working Practices Policy

8.9 Threatening or malicious comments are posted to the school website or social media about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

- Preserve any evidence and log the incident.
- Inform the Headteacher and e-Safety lead immediately.
- Check the filter if an Internet based website issue.
- Contact/parents and carers
- Refer to the anti-bullying policy
- Contact the police or CEOP as necessary.

8.10 If images or video of pupils engaged in sexual activity or in revealing poses (sexting) are known to have been posted online the following guidelines should be followed:

- Sexting is where young people share sexual images of themselves. Where this happens, images have usually been shared with a partner or intended partner as a form of flirtation or - in the eyes of the young person - 'safe sex'.
- This act itself poses a risk to the young person in the image: once it has been shared it is liable to be distributed further. This action may also place both the sender and the recipient in a position of having committed an offence under the Protection of Children Act 1978.Young people of an age likely to consider such actions should be educated about the risks. In the event of sexting Child Protection procedures should follow.

8.10a Your responsibilities when responding to an incident involving sexting

If you are made aware of an incident involving the consensual or non-consensual sharing of nude or semi-nude images/videos (also known as 'sexting' or 'youth produced sexual imagery'), you must report it to the DSL immediately.

You must **not**:

- View, copy, print, share, store or save the imagery yourself, or ask a pupil to share or download it (if you have already viewed the imagery by accident, you must report this to the DSL)
- Delete the imagery or ask the pupil to delete it
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery (this is the DSL's responsibility)

- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any young people involved
- You should explain that you need to report the incident, and reassure the pupil(s) that they will receive support and help from the DSL.

Initial review meeting

Following a report of an incident, the DSL will hold an initial review meeting with appropriate school staff – this may include the staff member who reported the incident and the safeguarding or leadership team that deals with safeguarding concerns. This meeting will consider the initial evidence and aim to determine:

- Whether there is an immediate risk to pupil(s)
- If a referral needs to be made to the police and/or children's social care
- If it is necessary to view the image(s) in order to safeguard the young person (in most cases, images or videos should not be viewed)
- What further information is required to decide on the best response
- Whether the image(s) has been shared widely and via what services and/or platforms (this may be unknown)
- Whether immediate action should be taken to delete or remove images or videos from devices or online services
- Any relevant facts about the pupils involved which would influence risk assessment
- If there is a need to contact another school, setting or individual
- Whether to contact parents or carers of the pupils involved (in most cases parents/carers should be involved)

The DSL will make an immediate referral to police and/or children's social care if:

- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example, owing to special educational needs)
- What the DSL knows about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the images or videos is under 13
- The DSL has reason to believe a pupil is at immediate risk of harm owing to the sharing of nudes and semi-nudes (for example, the young person is presenting as suicidal or self-harming)

If none of the above apply then the DSL,and other members of staff as appropriate, may decide to respond to the incident without involving the police or children's social care. The decision will be made and recorded in line with the procedures set out in this policy.

Further review by the DSL

If at the initial review stage a decision has been made not to refer to police and/or children's social care, the DSL will conduct a further review to establish the facts and assess the risks.
They will hold interviews with the pupils involved (if appropriate).
If at any point in the process there is a concern that a pupil has been harmed or is at risk of harm, a referral will be made to children's social care and/or the police immediately.

Informing parents/carers
The DSL will inform parents/carers at an early stage and keep them involved in the process, unless there is a good reason to believe that involving them would put the pupil at risk of harm.

Referring to the police
If it is necessary to refer an incident to the police, this will be done through dialing 101

Recording incidents
All incidents of sharing of nudes and semi-nudes, and the decisions made in responding to them, will be recorded and logged on CPOMS.

Curriculum coverage
Appropriate educational/pastoral work should be undertaken with all young people involved.

9.0 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 pupils' 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.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

10.0 Introducing the policy to pupils

- Rules for acceptable use will be posted in rooms where computers are used.
- Pupils will be informed that internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible internet use will be included in the Computing & RSHE schemes of work covering both school and home use.
- Oldham's youth charter may be displayed. (See appendix 2)

11.0 Introducing the policy to staff, governors and volunteers

- All staff, governors and volunteers must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.
- All staff including teachers, supply staff, teaching assistants, administration and site manager, kitchen staff, and Governors will be provided with the School Internet Policy, and its importance explained as part of their induction.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible internet use, including familiarisation of the E-safety and acceptable use agreement will be provided as required.

12.0. Parents

12.1 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.

12.2 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.

13.0 Data Protection - Managing and Storing Information

The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy. All documents stored are in accordance with legal requirements where appropriate, and guidance from the Records Management Toolkit for Schools. All records are kept confidential. Such records are retained for the length of time that the child remains at the school and then removed.
This policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level of Data Compliance Requirements
	✓	

14.0. Related policies

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

- Safeguarding and child protection
- Behaviour
- Staff Working Practices and Code of Conduct
- Data protection
- Remote learning

Appendix 1

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Ensure that the school has an effective filter and monitoring system for online learning and this is regularly reviewed.
This will be carried out by the Governors receiving regular information about e-safety incidents. The Governors role will include:

- updates from the E-Safety Lead
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policy / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Updates Governors to discuss current issues and review incident logs.
- Reports to Senior Leadership Team.
- Organises E safety week and Information events and keeps parents fully informed

Network Manager / Technical staff:
The IT technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

- That the use of the network / Internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / e-safety lead.

Teaching and Support Staff Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- They have read, understood and signed the Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the e-safety and acceptable use agreement
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Child Protection / Safeguarding Designated Person

The Child Protection Officer for the school should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their pupils understand the need to use the Internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, tweets, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to Twitter and the school website
- their pupil's personal devices in the school (where this is allowed)

Appendix 2

Oldham Charter of Young People's Digital Rights

Charter of Young People's Digital Rights

oldham Youth Council

1. You have the right to enjoy the internet and all the fun and safe things it has to offer.
2. You have a right to keep information about you private. You only have to tell people what you really want them to know.
3. You have a right to explore the internet but remember that you cannot trust everything that you see or read on the internet.
4. You have a right to know who you are talking to on the internet; you don't have to talk to someone if you don't want to.
5. Remember not everyone is who they say they are on the internet. You have a right to tell someone if you think anyone is suspicious.
6. You have a right NOT to fill out forms or not to answer questions you find on the Internet.
7. You have the right to NOT be videoed or photographed by anyone using cameras, web cams or mobile phones.
8. You have a right NOT to have any videos or images of yourself put on the Internet, and you have the right to report it to an adult if anyone does this.
9. You have a right NOT to be bullied by others on the Internet and you have the right to report this to an adult if this happens.
10. If you accidentally see something you shouldn't you have the right to tell someone and not to feel guilty about it.
11. We are ALL responsible for treating everyone on line with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

Oldham Youth Council 2008 - 2009

Launched in Oldham eSafety Week 2009. For more information and the interactive version of this charter, go to ***www.e-safetyweek.info***

Appendix 3

Contract for Acceptable Use of the Internet (Staff/Governor/Volunteer)

I know that I should only use school equipment in an appropriate manner.

I know that images should not be inappropriate or reveal any personal information of pupils and young people if uploading to the Internet.

I have read the school e-safety and acceptable use policy so that I can deal effectively with any problems that may arise.

I will report accidental misuse to the Headteacher.

I will report any incidents of concern for the pupil's safety to the Headteacher, designated person for child protection in accordance with the e-safety and acceptable use policy.

I know the designated person for child protection is Mrs Pamela Hartley and in her absence Mr Day

I will ensure that personal data (such as data held on SIMS) is kept secure and I follow the Data Protection Act .

I know that I am putting myself at risk of misinterpretation and allegation if I contact pupils and young people via personal technologies, including my personal e-mail and phone and should use the school e-mail and phones (if provided) and only to a child's school e-mail address if possible .

I will ensure that I keep my password secure and do not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will ensure that electronic communication with pupils and staff are compatible with my professional role.

Name: ……..

Signed:……..

Position:……..

Date:……

Appendix 4

Contract for Acceptable Use of the Internet (Pupil)

These rules help us to be fair to others and keep everyone safe.

I will ask permission before using the Internet.

I understand that I must not bring software or disks into school without permission.

I will only email people that my teacher has approved.

The messages that I send will be polite and sensible.

I understand that I must never give out my home address or telephone number, or arrange to meet someone.

I understand that I must ask for permission before opening an email or an email attachment sent by someone I do not know.

I will not use Internet chat.

If I see anything I am unhappy with or I receive a message I do not like, I will tell my teacher immediately.

I understand that the school may check my computer files and the Internet sites that I visit.

I understand that if I deliberately break the rules, I may not be allowed to use the Internet or computers.

Date: ……
The undersigned have read and agreed to the above.

Appendix 5

Incident log sheet

Person reporting incident:

Date:Time:

Action(s) agreed Contact eg telephone calls made
Please photocopy

Signed by adult raising the concern: ……

Signed by E-safety Lead: ……..

Appendix 6

Information and websites about e-safety.

CEOP

• http://www.ceop.gov.uk

Think U Know

• http://www.thinkuknow.co.uk/Default.aspx?AspxAutoDetectCookieSupport=1

Becta

• http://localauthorities.becta.org.uk/index.php?section=esf

Childnet

• http://www.childnet-int.org

Internet Watch Foundation

• http://www.iwf.org.uk

BBC

• http://www.bbc.co.uk/cbbc/help/web/staysafe

Appendix 7

St Mary's C of E Primary School guidance note on privacy settings within social media sites and apps.

This document is intended as a guidance note on "how to" maintain your privacy within the "top 3" social media environments readily used by people on a day to day basis and is a **supplementary note to the Safer Working Practices Policy – specifically section *" Social Contact and Social Networking".*** The note is based on advice and guidance from a few different sources including the NASUWT and the University of Sussex.

Facebook

Facebook is the number one social media site platform across the world. As of the second quarter in 2015, Facebook has just under 1.5 billion active users, of which over 1 billion use on a monthly basis at least. The points below are suggested guidance on how to maintain a level of privacy with a Facebook profile and the information contained within it.

It should be noted that the legal minimum age to have a Facebook profile within the UK is **13**.

The NASUWT recommend that:

1. To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly (see below)
2. Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school.
3. Always make sure that you log out of Facebook after using it, particularly when using a machine that is shared. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window).

To maintain your privacy, they recommend the following settings are enabled: **NB: If you choose to enable any or all of the recommendations described below, this must be done in the web version of Facebook, NOT via the smartphone/tablet app.**

Privacy Setting	Recommended Security Level
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you're tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check in to	Friends only
Contact information	Friends only

Even when the privacy settings are set to 'friends only', you might be surprised to see some information still readily available to the public via a "Google" search on your name and then people still being able to link to your Facebook profile and view:

1. previous posts (pre-privacy settings)

2. previous Facebook banners
3. your friends block
4. groups you have recently joined
5. your relationship status (if published)
6. the 'about you' block
7. recent activity

In order to prevent this, the University of Sussex recommend applying the following additional privacy settings:

1. Go to **Settings**
2. Select **Privacy**
3. Change all of your posts to be available **only to friends** (as described above)
4. Set **'delete past posts'** to ensure posts that were public before your settings changed are deleted from your timeline.
5. Then go to **Manage Sections.** You will find this in the top toolbar. Untick all of the options so that no blocks are available for public viewing.
6. And finally…go to your photo block (and other blocks including groups block, friends block, etc) and click on the **edit pencil** and select **hide**.

Last thing, make sure your banner and your personal profile picture is an image with information that you wish to share. No matter what your settings, **these two images will be available at all times.**

If you choose to apply these settings, you can check how your profile will appear once this is completed by:

1. go to settings
2. go to **view as**
3. select 'public' view

This will provide you with a view of your profile as it will appear to someone how finds you within a "Google" search and how is not currently within your "Facebook Friends List".

It's useful to note that Facebook changes its privacy settings from time to time so what might have been private yesterday could be public tomorrow. A new feature was added by Facebook on the 17th of September; a friendly dinosaur that can help you with your privacy settings, available under your privacy shortcut.

Instagram

Instagram is the second most used social media platform across the globe with a disclosed total number of 400 million active users, of which 75 million use the platform on a day to day basis. Like Twitter, by default an Instagram profile is "public" – i.e. whatever images you post can be seen by any other Instagram user (whether you have approved them as a follower or not) or via a simple search on the internet.

Like Facebook, Instagram does have a legal minimum age of 13.

The notes below provide some guidance/pointers on how to enable a level of security on your Instagram profile.
NB: these changes can [and should] be applied via the Instagram app, unlike Facebook and Twitter.

1. Open the Instagram app on your smartphone or tablet.
2. Go to your profile by touching the "person" button in the lower right-hand corner.
3. Touch the "wheel" (or "cog") image in the top right of your screen.
4. Under the account section, Switch to On the "Private Account" setting.
5. Upon clicking Instagram will ask for confirmation.
6. Confirm it by touching "YES".

From now on anyone who wants to see your Instagram photos has to send you a follow request which will appear in the news feed. To check who has requested to follow you and either approve or ignore, then:

7. Go to the news/activity feed by clicking the feed icon on the bottom [A speech bubble with a heart inside it].
8. You will reach the news/activity feed where you'll see a "follow requests" section at the top.
9. If you have multiple requests, the number will be displayed and on clicking on this, a list will form.
10. You can then "approve" [Green Tick] or "ignore" [Red Cross] each request.
11. If you have a single request, the "approve" or "ignore" options will appear directly within the news/activity feed.

Linking Instagram to other social media platforms.

Some websites, social networks and apps give you the option to sign in or to verify your identity by linking your account to their service. Whilst this is OK, you should be aware that you're giving the third party (the website, social network or app) access to your Instagram username, your lists of followers, who you are following, and your location (if you share it) and your posts - even if you've set them to "Private".

Twitter

Twitter is the third most used social media platform across the world and has a significantly smaller user base across the planet – as at the end of Sept 2015, it had 232 million active users. By default, a Twitter profile is "public" – i.e. whatever you tweet can be seen by any other Twitter user (whether you have approved them as a follower or not) or via a simple search on the internet. The notes below provide some guidance/pointers on how to enable a level of security on your Twitter profile.

Unlike Facebook & Instagram, there is NO legal minimum age for the use of Twitter, but the recommended minimum age is 13. Your date of birth is not required to create a Twitter account.

It should be noted that by making your profile and Tweets private the following will apply:

1. Other users will need to make a request to follow you, and you will need to approve all requests.
2. Your tweets will only be visible to approved followers.
3. Other users will be unable to retweet you.
4. Your tweets will not appear in any Google searches, and will only appear in Twitter searches conducted by your approved followers.
5. Any @replies you send will not be seen, unless you send them to your approved followers. For example, if you tweet a celebrity they will not be able to see it, unless you have approved them to follow you.
6. Anything you tweeted while your account was public will now become private, and will only be viewable or searchable by your approved followers.
7. You will only be able to share permanent links to your tweets with your approved followers.

If you wish to enable privacy on your Twitter account (which is recommended) then the following steps need to be applied via the webpage version of your account:

- Log in to your Twitter account with your username and password and click on your profile picture and select "settings". Under settings, select "security and privacy". **Then click [check] the following boxes:**
  - **Photo Tagging:** Do not allow anyone to tag me in photos Though others can still upload photos of you, you now can't be publicly tagged in them.
  - **Tweet Privacy:** Protect My Tweets People will now need your permission before they can follow you (though you will keep all the followers you have now). Future tweets will only be visible to your followers, no-on can retweet your tweets, and your tweets will not show up in Google search results Limitations: you can't reply to tweets posted by non-followers. **Note:** this only works on future tweets; all past tweets will still be public.
  - **Discoverability**: Let others find me by my email address People now can't find your Twitter account by searching your email address. This is especially if you do not want your email address publicly linked to your account.

Linking Twitter to other social media platforms.

As with Instagram, you can link or share your Tweets via other social media platforms, however, the same cautionary note applies, in that you're giving the third party (the website, social network or app) access to your Twitter username, your lists of followers and following, and your location (if you share it) and your tweets - even if you've set them to "Private". You will also be giving Twitter information about the other services that you use.

With all this in place finally think about the content of what you post, any content should not bring the school or the profession into disrepute.