ST. PATRICK'S R.C. PRIMARY SCHOOL

ONLINE SAFETY POLICY

Date Policy Approved:	March 2021
Date Approved by Governors:	March 2021
Date of Next Review:	Spring 2023

ONLINE SAFETY POLICY

Our Mission

We come to a Roman Catholic School and so believe that Jesus was born, died and rose again for everyone. We aim to help, encourage and show God's way to our families, making sure that our Catholic traditions and faith are kept alive. Each year at school, we learn a little bit more about our faith so that we can all grow to love God and each other more.

At St. Patrick's, we seek at all times to be a witness to Jesus Christ. We remember this when putting our policies into practice.

1. Aims

Our school's aim is to:

- Have robust processes in place to ensure the online safety of pupils, staff, supply teachers, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Our school will offer a supportive environment where children, staff, parents/carers and governors feel valued respected and happy.

2. Background/Rationale

New technologies have become integral to the lives of children and young people in society, both within school and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access.

The requirement to ensure that children and young people can use online and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school's online safety policy will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The risk of being targeted by extremists in order to promote and encourage radicalisation;
- The risk of being targeted by those involved in child sexual exploitation;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyberbullying;
- Access to unsuitable video/internet games;

- An inability to evaluate the quality, accuracy and relevance of information on the Internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies including the Safeguarding & Child Protection, Data Protection and Whole School Behaviour.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

3. Associated School Policies and procedures

This Policy should be read in conjunction with the following school policies/procedures and, where they exist, addendums to those policies and procedures:

- Safeguarding & Child Protection Policy and procedures
- Data Protection Policy
- Health and Safety Policy and procedures
- Whole School Behaviour Policy
- Whistleblowing procedures
- Code of Conduct for staff and other adults
- Home-School Agreement

Communication/Monitoring/Review of this Policy and procedures

This policy and procedures will be communicated to staff, pupils and the wider community in the following ways:

- Posted on the school website/shared staff drive
- Policy and procedures to be discussed as part of the school induction pack for new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be held in pupil and personnel files

The online safety policy is referenced from within other school policies and procedures as outlined above.

4. Scope of the Policy

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

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers in relation to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken in relation to issues covered by the published behaviour policy and procedures.

The school will deal with such incidents within this policy and procedures and the whole school behaviour policy which includes anti-bullying procedures and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

5. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study.

6. Roles and responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

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

The Executive Headteacher

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

The Designated Safeguarding Lead

The overall responsibility for Child Protection and online safety lies with the Executive Headteacher, however, a team of Designated Safeguarding Leads support with this.

Safeguarding is a serious matter; we use technology and the internet across all areas of the curriculum and ensure that it is comprehensive, age-related and effective. Online safeguarding, known as online safety, is an area that is constantly evolving. At our schools, we ensure that staff online safety CPD is current and included in staff induction; as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

Details of the school's Designated Safeguarding Leads (DSL) are set out in our safeguarding and child protection policy.

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

- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Headteacher, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Headteacher and/or governing body

This list is not intended to be exhaustive.

The Computing Lead

The Computing Lead, alongside the IT Technician, is responsible for:

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

This list is not intended to be exhaustive.

All staff (including supply staff and volunteers)

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

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

This list is not intended to be exhaustive.

Parents/Carers

Our school uses a Digital Platform called ClassDojo, which is a social online space for teachers and parents/carers to share learning both at home and in school. The site is completely secure, and every parent has an individual username and account- the majority of parents/carers utilise their account. All pupils sign an agreement at the beginning of each school year to show they are agreeing to follow the rules regarding online safety. Anyone not following the rules for online safety will be dealt with in line with our behaviour policy.

Parents/carers are expected to:

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

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents/carers-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents/carers-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents/carers-factsheet-09-17.pdf

Digital Images

Parents/carers sign an annual consent form for the use of images of their children for school purposes and on the internet: the school website, ClassDojo, social media etc. - the child's name is never included with their image. Digital images may be shared with partner schools and organisations as part of collaborative learning projects. All such use is monitored and supervised by staff.

Visitors and members of the community

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

7. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, addressed primarily through Computing and PSHE teaching and learning as well as other opportunities across the curriculum.

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

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

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

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

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

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

Email Safety

We do not allow pupils to send emails externally. Via the Computing curriculum, they are taught how to use email safely and how to communicate appropriately through email. Staff use the G-Mail e-mail system, and this should only be used for school purposes.

8. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website, school Facebook page and newsletters This policy will also be shared with parents/carers.

Online safety will also be highlighted during parents' evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher. Concerns or queries about this policy can be raised with any member of staff or the Executive Headteacher.

9. Cyber-bullying

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.)

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. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies. 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.

All staff, governors and supply staff & 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).

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.

10. Acceptable use of the internet in school

Pupils' Access to the Internet and Network Safety

All users log on to the network using a personal username and password. On the network, there are different areas where groups of users can save work so that it is available to others. Pupils are taught how to access and save to shared resource areas. Teachers sometimes use the network to share files with each other; children do not have access to these files.

When using networked equipment, all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually block site addresses which are considered to be unacceptable. However, no system is 100% safe, and pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive or which introduce software which can damage the equipment. No-one must attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media. We have an online safety curriculum, integrated into our Computing curriculum, which has been designed to teach the children how to keep themselves safe whilst using the internet. We also cover this issue annually during our Anti-Bullying week and regular assemblies.

Pupils accessing the internet at home are subject to the controls placed upon them by their parents/carers. To support parents/carers in safeguarding their children, on the school website we publish specific advice for parents/carers with regards online safety and how best to protect their child in this respect. We also share this advice via newsletters on a regular basis. However, any home use of the Internet made in connection with the school or school activities will be subject to this policy and any breach dealt with as if the event took place at school.

All pupils, parents/carers, staff, supply staff & volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). 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, supply staff & volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the acceptable use agreements in appendices 1 and 2.

11. Pupils using mobile devices in school

Pupils are not allowed mobile phones or personal electronic devices in school - any such items brought in must be handed in to the office and returned to parents/carers at the end of the day.

Mobile devices belonging to staff should not be used to store children's personal data. No personal data such as home addresses, contact telephone numbers, medical information or photographs should be kept on such devices. Mobile phones and personal devices should not be used in teaching areas.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

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

12. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Computing Lead/ IT Technician.

Work devices must be used solely for work activities.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

The Executive Headteacher / Designated Safeguarding Leads / Computing Lead will ensure these procedures are followed by staff in the event of any misuse of the internet:

An inappropriate website is accessed inadvertently:

- Report website address to the Computing Lead by logging the incident on CPOMS and alerting them.
- The Computing Lead then contacts ICT Technical Support to amend school filters as necessary.

An inappropriate website is accessed deliberately:

- Report website address to the Computing Lead by logging the incident on CPOMS and alerting them.
- The Computing Lead then contacts ICT Technical Support to emend school filters as necessary.
- Decide on appropriate action.

An adult receives inappropriate material:

- Do not forward this material to anyone else.

Report to the Computing Lead by logging the incident on CPOMS and alerting them.

- Contact relevant authorities for further advice e.g. police, social care, CEOP.

An illegal website is accessed or illegal material or evidence of illegal activity is found on a computer:

This may contain racist, obscene or violent materials.

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

- Alert the Executive Headteacher / DHT/Computing Lead immediately.
- DO NOT LOG OFF the device but do bring it to be kept in a safe place.
- Contact the police / CEOP and social care immediately.
- If a member of staff, supply teacher or volunteer is involved, refer to the Whistleblowing Policy and report to the Local Authority Designated Officer.

Threatening or malicious comments are posted to the school's digital community- Facebook-about an adult or child in school, or in the instance that malicious text messages are sent to another child/young person (cyber bullying):

- Preserve any evidence and log the incident on CPOMS and alerting the appropriate people.
- Inform the Executive Headteacher/DHT immediately and follow Child Protection Policy.
- Inform a Designated Safeguarding Lead.
- Check the filter if an internet-based website issue.
- Contact/parents/carers and carers.
- Contact the police or CEOP if appropriate.

14. Training

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, weekly staff bulletins, notices on the staff noticeboard and staff meetings).

The DSL 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.

Supply staff & volunteers will receive appropriate training and updates, if applicable.

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

15. Monitoring arrangements

Behaviour and safeguarding issues related to online safety are logged using CPOMS.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing body.

16. Links with other policies

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
- Remote Learning Plan and Policy

17. Remote/ Home Learning

We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' in the circumstance of a class/whole school having to isolate by providing a range of resources via our website and an appropriate e-learning portal. We expect pupils to follow the same principles, as outlined in the school's Acceptable Use policy, whilst learning at home. In line with our Remote Learning Plan and Policy, if the school chooses to communicate with pupils over the coming weeks/months via Zoom, Teams, Skype etc. then it is important that this is only carried out with the approval of the Executive Headteacher or Deputy Heads.

Pupils must uphold the same level of behavioural expectations as they would in a normal classroom setting. Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.

Staff should be mindful that when dealing with any behavioural incidents online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents/carers, regardless how minor the incident, to ensure the child is emotionally well supported.

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

Acceptable Use of ICT Agreement

When I am using the computer or other technologies, I want to feel safe at all times.

I agree that I will:

KEEP SAFE:

- I will always keep my password secret.
- I will choose usernames carefully to protect my identity.
- I will only visit sites which are appropriate to my work at the time.
- I will only email people I know or those approved by a responsible adult, such as my parents/carers or my teachers.
- I will always keep my personal details private. (My name, family information, my journey to school and home from school, my birthday or year of birth)
- I will always check with a responsible adult or my parents/carers before I show any photographs of myself.
- I will never meet an online friend without taking a responsible adult, such as my parent or grandparent with me.
- I will ask my parent/ care before adding people as friends on online games and consoles.

COMMUNICATE RESPONSIBLY:

- I will make sure all messages I send and comments I submit are respectful, necessary and will promote the Gospel values that we live by at St Patrick's.
- I will not reply to any nasty message or anything that makes me feel uncomfortable or scared.
- I know that once I post a message or an item on the Internet then it is completely out of my control and even if I delete it, it may still be available to others.

TAKE CARE BEFORE I SHARE:

- I will not give my mobile phone number to anyone who is not a real friend.
- I will always check with my parents/carers or teachers if I can upload photographs.

REPORT PROBLEMS:

- I will tell a responsible adult straight away if anything online makes me feel scared or uncomfortable.
- I will show a responsible adult if I get a nasty message or receive anything that makes me feel uncomfortable or afraid.

Signed (Child)…… Signed (Parent/Carer)……

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

All staff are expected to sign this policy and adhere at all times to its contents.

- I will always log off my computer/lap-top when I finish using it.
- I will always put a security lock (ctrl/alt/delete) on when I leave my computer/laptop unattended.
- I will take the necessary care of any school-issued device and understand that it is my responsibility to look after it.
- I will ensure that I have the adequate and appropriate home insurance if I take the school-issued device home.
- I will only use the school's email, internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher and Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that I adhere to and comply with the school's data protection policy.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that I comply with the school's data protection policy when handling any personal data and ensure that all schoolwork is undertaken on a school issued device or an encrypted USB.
- I will ensure that I comply with the school's whistleblowing policy and follow the necessary procedures if I have concerns about another member of staff and their use of IT.
- I will not share my password with colleagues, pupils or parents unless at the request of the Executive Headteacher or Governing Body for investigation purposes.
- I will not install any hardware or software.
- I will not browse, download, upload, or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, guardian or staff member. Images will not be distributed outside the school network without permission of the parent/guardian, member of staff or Executive Headteacher.
- Images of pupils and/or staff will be deleted once they have been used for purpose.
- I understand that all my use of the internet and other related technologies is monitored and logged and can be made available, on request, to the Executive Headteacher or governing body.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand that email or text communication with a child outside of agreed protocols, may lead to disciplinary and/or criminal investigations.
- I have read and understand and agree to adhere to 'Keeping Children Safe in Education' part 1(September 2020).

In addition:

- I will not have any communication with pupils on social networking sites. Although you may not be close to a person on your 'friends' list the connotation of the word friend is strong and this must be considered when making a choice on who to accept.
- I understand that the Governing Body strongly advises that I do not have communication with any parents from our schools on social networking sites.
- I will keep up to date with the latest guidelines, policies and procedures for Acceptable-use, online safety and social media.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Personal publishing and on-line communication will be taught via age appropriate sites that are suitable for educational purposes. They will be monitored by the school.
- All members of the school community, in line with other policies are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- News groups will be blocked unless a specific use is approved.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/guardians who will be reminded of our online safety policy.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.

Staff use of personal devices:

- I will ensure I follow school policy regarding how and when I use my mobile phone to access my school email account, Facebook, twitter and CPOMs.
- I will be the only person to access these accounts from my phone and I will ensure I have the necessary security and settings in place.
- I will ensure that when accessing these accounts, I am doing so for school business and I am away from other people.
- I fully understand the implications if I choose to have access to these accounts from my phone.
- I will not use my own personal phone or device for contacting children, young people and their families within or outside of the setting in a professional capacity.
- I will use the school phone where contact with pupils or parents/guardians is required.
- I will not provide any child with my personal contact details including my mobile telephone number.
- I will not request, or respond to, any personal information from a child other than that which is appropriate as part of my professional role.
- Once in school, I will switch my mobile phone and device to "silent" mode and bluetooth communication should be "hidden" or switched off.
- I will not use my mobile phone or other personal IT devices during working hours/contact with children unless permission has been given by the Executive Headteacher or in her absence one of the Deputy Headteachers in emergency/extenuating circumstances.
- My mobile phone will not be kept about my person, i.e. in my pocket or at my work station during working hours. I will put it somewhere safe (class stock room, school office, staff room, office drawer) and out of reach of pupils.
- I will not use any personal device such as a mobile phone or camera to take photos or videos of pupils and will only use school-issued equipment for this purpose.
- I understand that if I choose not to adhere to this policy, then disciplinary action may be taken.

List of social media sites that staff will access for curriculum and school use:

- Facebook
- Twitter
- Instagram
- Snapchat
- Tik Tok

User Signature

I agree to follow this Online Safety & Acceptable Use policy and support the safe and secure use of IT & personal data throughout the school. I understand my responsibility and the accountability.

Staff signature _____ Date _____

Full name _____ (printed)

Appendix 3: Online Safety Training Needs – Self-Audit for Staff

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