St Marie's Catholic Primary School

E safety Policy

'The Love of Christ, nurture, guide and inspire us.'

Approving Body	Full Governors Committee Head/Leadership team	**Review Term: 1yr/2yr/3yr** Autumn Spring Summer
Signature:	Chair of the relevant body	**December 22**
Review Date:	March 24	**Version:** (applicable if changed within the review period, if no changes this would remain as version 1)

MISSION STATEMENT

'The Love of Christ, nurture, guide and inspire us.'

To do this we will:

- Be a Christian community that lives the Gospel values; 'Love of Christ' (Christ centred)
- Provide opportunities for all to grow and achieve by igniting a desire for learning; 'Guide and inspire' (Education)
- Be a haven of peace and love that enables all to thrive; 'Nurture' (Community)

Objectives: Christ Centred

- Provide high quality collective worship and enriching liturgical celebrations
- Enable our children to acquire an excellent religious education and develop their relationship with God
- Share faith, love and hope in the likeness of Mary, Mother of God
- Provide a safe harbour where all can succeed

Objectives: Education

- Have high expectations of ourselves and others in all that we do
- Value our pupils and staff, appreciating their uniqueness and individual talents, enabling them to achieve well
- Provide a curriculum that opens the world, in all its awe and wonder, to our pupils

Objectives: Community

- Create a peaceful, happy school where all feel welcomed and valued
- Nurture and grow our pupils and community in the Gospel values
- Celebrate each person as a beautiful work of art, created on God's image

St Marie's Key Objectives and Priorities 2023/2024

Key Objectives and Priorities	Success Criteria
Christ at the Centre 1. Priority: Culture	• Ensure that staff and pupils are clear on whole school expectations, routines and behaviours • Pedagogy, policies and procedures are shared and implemented with fidelity • Relationships across the school community become strong • Staff seek every opportunity to promote learning within and beyond the school day • Pupils and staff have the tools needed to ensure resilience in their learning and wider lives
2. Priority: Aspiration	• School has unapologetically high aspiration for our children through a fully understood, common pedagogy • All children can access a low floor-high ceiling, fully resourced, holistic curriculum that meets our high aspirations which staff are equipped to deliver • Percentage of children at greater depth standards is rapidly closing the gap with national
3. Priority: Resources	• The staff structure, skills and knowledge meet the needs of the school • 'The curriculum' is fully resourced and meets the needs of our children with effective schemes of work, curriculum knowledge and skills progression maps • All staff receive high quality assured CPD that improves learning for all pupils
4. Priority: Community	• Parents are well equipped to support children learning in school and at home • Families are well supported to meet our aspirations for our children, i.e. through uniform and attendance • Our community is well involved in school life, e.g. Parent Council, FAF group etc
5. Priority: Environment	• The school building and grounds are a safe place to work and play • The buildings and classrooms promote our high aspirations

Revision	Date	Author	Summary of Changes
V1.0	May 2015	Maria Bannister Information Technology Client Manager: Schools	Replaces previous eSafety Strategy issued 2010. Produced for consultation.
V2.0	September 2015	Maria Bannister Information Technologies Client Manager: Schools	Includes recommendations from consultation process, guidance on the "Prevent Duty" and Social Media AUP for pupils

In Consultation with:
Maria Taylor – Strategic Lead for Education
Andy Garden – Head of IT
David Norton – Principal HR Manager on behalf of Dave Turner: Head of HR
Alan Johnson – Senior Solicitor on behalf of Mike Dearing: Head of Legal

Adopted by Schools Information and Technologies Strategic Board

Date: March 24

Version: 2.0

Distribution: All Primary Schools, Special Schools and Centres for Learning.

School eSafety Policy

Contents

Glossary of Terms

Blogging & Social Networking: Web 2.0 technologies which enable the creation and distribution of content with like-minded people. A powerful network for sharing ideas and influencing opinion.

BYOD: Bring Your Own Device – approved use of personally owned devices on the school network.

Cloud: A service were information, pictures, videos and other media can be stored on a remote server and accessed via the internet by a single person or shared with a group of people.

Copyright: The exclusive legal right of the originator of print, publish, perform, film or record literary, artistic or musical material.

Cyberbullying: the use of ICT (information and communications technology – particularly mobile phones and the internet) to deliberately upset someone else.

Digital Natives: those born into and raised in the digital age.

Digital Citizenship: appropriate and responsible behaviour with regard to use of technology.

Digital Footprint: the term used to describe the trail, traces or "footprints" that people leave online. This is information transmitted online, such as forum registration, e-mails and attachments, uploading videos or digital images and any other form of transmission of information — all of which leaves traces of personal information available to others online

Downloading: receiving information electronically through the internet. This could include saving a document or picture from a website or media streaming e.g. music or video.

eSafety: The process of limiting risks to children and young people when they are using ICT. It is primarily a safeguarding issue and relates to all ICT fixed or mobile technologies, software, content and the internet or cloud services.

eSafeguarding: a safeguarding issue where technology is involved

Extremism: defined in the 2011 Prevent strategy as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. Also included in the "Prevent" definition of extremism are calls for the death of members of our armed forces, whether in this country or overseas.

Filtering: software that can block access to specific websites and/or inappropriate material. No filtering can guarantee to be completely effective and other strategies including education and awareness raising need to be applied.

Firewall: a buffer between the computer and the internet which regulates both incoming and outgoing information.

Frape: hacking of online profiles

Grooming: building an emotional connection with a child to gain their trust for the purpose of sexual abuse or sexual exploitation

Hacking: when personal details, online accounts or other personal information is accessed without your permission and prior knowledge.

ICT: Information and Communications Technology for example, mobile phones, tablet devices, gaming consoles, email and social networking

Identity theft: when your personal information is used by someone else without your knowledge.

LADO: The role of the Local Authority Designated Officer is defined in the HM Guidance "Working Together to Safeguard Children (2013). The LADO is appointed by the Local Authority to manage allegations that a person who works with children has behaved in a way that has harmed, or may have harmed, a child, possibly committed a criminal offence against children, or related to a child or behaved towards a child or children in a way that indicates s/he is unsuitable to work with children.

Netiquette: Netiquette, or net etiquette, refers to etiquette on the Internet. Good netiquette involves respecting others' privacy and not doing anything online that will annoy or frustrate other people. Three

areas where good netiquette is highly stressed are e-mail, online chat, and newsgroups. For example, people who spam other users with unwanted e-mails or flood them with messages have very bad netiquette. You don't want to be one of those people. If you're new to a newsgroup or online chat room, it may help to observe how people communicate with each other before jumping in.

Other stakeholders: includes staff, students, pupils, volunteers, parents, carers, visitors, community users and guests

Phishing: Phishing refers to fraudsters who send spam or pop up messages with the intention of getting information from people.

Radicalisation: refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Sexting: sending and receiving of personally intimate images – also referred to as SGII (selfgenerated indecent images)

Spam: Spam refers to emails advertising products for sale online or any unsolicited and/or irrelevant which are sent to a large number of recipients without their consent. Spam can be malicious with the intent to spread computer viruses and/or malware.

Spyware and Adware: general term to describe software designed to take control of a device without the permission of the user. Adware refers to commercial adverts shown to the recipient without their consent.

Uploading: sending or saving information from a local system or device e.g. mobile phone or computer to a remote system i.e. website.

URL: Universal Resource Locator – the unique address for a website.

Video Chat: Face to face conversation held over the internet by means of webcams and dedicated software.

VoIP: Voice Over Internet Protocol – transmission techniques involved in the delivery of voice communications and multi-media sessions over networks including the internet.

Information and organisations:

CEOP: The Child Exploitation and Online Protection Centre. Part of the Police they work to protect children from sexual abuse linking with international partners when required. CEOP develop and deliver resources to inform and educate about risk through the *Think U Know* educational programme.

Childnet: organisation that works in partnership with others to make the internet a safer place for children.

Internet Watch Foundation (IWF): Organisation that takes reports about illegal online content and are the "notice and take down" body for any content within their remit. Work in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of content: child sexual abuse content anywhere in the world and criminally obscene and racial hatred content in the UK.

UK Safer Internet Centre (UKSIC): Partnership of three organisations: Childnet International, Internet Watch Foundation and South West Grid for Learning – three main functions: Awareness Centre, Helpline and a Hotline.

Acknowledgements and References:

Born Digital: Understanding the First Generation of Digital Natives – John Palfrey and Urs Gasser

Becta: Safeguarding Children in A Digital World (Developing a LSCB eSafety Strategy)

London Grid for Learning

Kent County Council Department for Education

Useful links:

Search and confiscation guidance from DfE:

https://www.gov.uk/government/publications/searching-screening-and-confiscation

Prevent Duty Guidance: https://www.gov.uk/government/publications/prevent-duty-guidance

Becta: Safeguarding Children in a Digital World:

http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/BEC1-15535.pdf How to hide your telephone number:

http://www.wikihow.com/Hide-Your-Phone-Number-(UK)

1.0 Introduction and overview:

Palfrey and Gasser in their book "Born Digital" say that anyone born after 1980 can be considered a digital native – part of the first generation born with access to digital technologies and the knowledge how to use them. Unlike 'digital immigrants', 'digital natives' live much of their lives online, without distinguishing between the online and the offline. Instead of thinking of their digital identity and their real-space identity as separate things, they just have an identity and they feel as comfortable in online spaces as they do in offline ones. The revolution in technology means that our children and young people are able to access information with immediacy and work collaboratively - the learning opportunities are tremendous. Digital natives are increasing coming to rely on this shared space for all the information they need to live their lives.

However, they inject a note of caution about some aspects of the way in which digital natives lead their lives saying digital natives have different ideas about privacy from those of their parents and as a result of spending so much time online, they are leaving more traces of themselves in publicly accessible places. In some cases, their online presence will show who they are and what they aspire to be – at worst they put information online that may put them in danger or compromise them in the future. Whether we are digital natives or digital immigrants, we all have a responsibility to create an online environment that is accessible, informative, creative, responsible and safe. We have a duty to be supportive of each other in our online lives. For some of us this is a professional responsibility – for all of us it is a moral duty. We need to develop and sustain an esafety culture. This and other linked policies underpin this objective.

1.1 What are the risks?

While recognising the enormous potential of technology and its applications, we need to accept that there are associated risks and develop effective mitigating strategies to address them. Different challenges will present on an ongoing basis but the main risks can be considered to fall within specific categories. Ofsted classify these three categories as:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being exposed to harmful online interactions with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

(Ref: Ofsted 2013)

Content: child as recipient			
Commercial	**Aggressive**	**Sexual**	**Values**
Adverts Spam Sponsorship Personal information	Violent/hateful content Grooming Cyberbullying (in all forms)	Pornographic or unwelcome content Exposure to inappropriate content including pornography, violence (often with offensive language), substance abuse and age restricted gaming	Biased, racist or misleading information or advice Hate sites Content validation: checking the validity and accuracy of online content
Contact: child as participant			
Commercial	**Aggressive**	**Sexual**	**Values**
Tracking Harvesting personal Information Identity theft (including frape) and sharing passwords	Being bullied, harassed or stalked	Meeting strangers or being groomed	Self-harm Unwelcome persuasions Lifestyle websites (including proanorexia, self-harm, suicide)
Conduct: child as actor			
Commercial	**Aggressive**	**Sexual**	**Values**
Illegal downloading Hacking Gambling Financial scams Terrorism Privacy issues – including disclosure of personal information Digital footprint and online reputation	Bullying or harassing someone	Creating and uploading inappropriate material including sexting	Providing misleading advice or information Health and wellbeing (amount of time spent online – internet or gaming) Copyright issues – intellectual property and ownership related to music, film and images

Developed by EU Kids Online Project - Adapted locally for this policy.

1.2 What is eSafety?

eSafeguarding, internet safety, esafety, digital safeguarding and online safety are interchangeable but all relate to ensuring that those who use technology do so safely and responsibly. Typically, esafety tends to be associated with online grooming, cyberbullying or access to inappropriate images/video. However, there is a broader and developing agenda related to the growth of social media including information

privacy, sexting, self-generated indecent content, gaming addiction, radicalisation and others. eSafeguarding is a common thread running across related areas including child sexual exploitation, anti-bullying and anti-social behaviour. In recent times there has been a prolific social media campaign (which experts assess to be widespread and highly advanced) by violent and brutal extremist groups such as Islamic State, to disseminate extremist views and groom potential adherents. The use of social media to engage and incite potential followers is a new phenomenon, changing traditional notions of how terrorist and cult groups communicate and leading to children and young people being exposed to extremist content in the online world. This threat of exposure to extremism does not just come from groups such as Islamic State but also from 'far-right' groups. As a result, the scope of e-safety and safeguarding has changed, with new and unprecedented online threats posed to children across the UK from this radicalisation and extremism activity.

Children and young people have the aptitude to use technology, but don't necessarily have the awareness, experience and knowledge to do so safely. We need to view the technology from the perspective of the child and take account of how their social lives (and therefore emotional development) are tied up in technology. We cannot, therefore, consider safeguarding and wellbeing without considering the relationship with technology and we must be careful to balance the risks with the advantages and opportunities.

The collective term esafety is used throughout this document to encompass the safe use of all online technologies.

1.3 Scope of the policy and the legislation:

Schools and further education institutions have a duty to safeguard and promote the welfare of pupils under the Children Act 2004 and Education Act 2002. These acts place a duty of care on schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Sections 90 and 91 of the Education and Inspections Act 2006 provide statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 also gives schools the power to confiscate items from pupils if they suspect they are being used in a way that is compromising to the wellbeing or safety of others. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices. These powers are particularly significant when dealing with incidents of cyber-bullying or other esafety incidents which take place outside the school. Action can only be taken under the acts where such issues are covered by the published behaviour policy. Schools should consider their legal powers when writing policies and procedures and document sanctions for breach of policy accordingly. The Counter Terrorism and Security Act 2015 includes a duty for schools to have due regard to the need to prevent children and young people being drawn into terrorism. Guidance stipulates that schools have a vital role to play in protecting children from extremism and radicalisation and risks posed through terrorist exploitation of social media should be approached in the same way as dealing with other forms of online abuse.

1.3.1 Ofsted:

From September 2014 Ofsted significantly reduced the amount of guidance it publishes for inspectors, schools and other stakeholders. As of January 2015, there are three guidance documents:

- The Framework for School Inspection
- School Inspection Handbook
- Inspecting Safeguarding in Maintained Schools and Academies

As part of the behaviour and safety judgement inspectors will consider the effectiveness of safeguarding arrangements to ensure that there is safe recruitment and that all pupils are safe. This includes the promotion of safe practises and a culture of safety, including e-safety. The school will also be measured on the effectiveness of the school's actions to prevent and tackle all forms of bullying and harassment including cyberbullying. Inspectors will also consider e-safety arrangements and actions taken following any serious safeguarding incident. In an outstanding school pupils are not only safe, they feel safe. They understand what constitutes unsafe situations and are aware how to keep themselves and others safe in different situations. This includes staying safe when using technologies.

1.4 Strategic approach – BECTA Pies Model:

This strategy is based on the BECTA PIES Model:

Ref: Safeguarding Children in a Digital World (Becta 2008)

The model works on the principle that effective policies and practises, education and training and a robust infrastructure (all of which are regularly monitored, reviewed and adapted as necessary) will support an effective approach to esafety. There is no panacea to the challenges and while every effort can be made to mitigate risk – it may not be possible to completely eliminate it. In circumstances where all reasonable measures fail to prevent an incident, effective policies ensure protocols are in place to deal quickly with consequences and ensure children continue to be protected. There is no single solution - a number of approaches (that support and complement each other) need to be applied. Fundamental to all of this is the recognition that esafety is not an ICT issue – it's a safeguarding one!

1.4.1 Policies and practises:

Safer management through effective policies, procedures and practices - as a minimum schools should:

- ✓ Appoint a dedicated esafety Lead
- ✓ Create and maintain an esafety Policy
- ✓ Make sure that appropriate Acceptable Use Policies and Staff User Agreements are in place.
- ✓ Have a reporting procedure in place that takes account of the approach that will need to be taken when reporting: i. misuse, ii. risk of harm
- ✓ Review and evaluate all internal policies at least annually or sooner in response to new technologies, developments, threats or incidents.

1.4.2 Infrastructure and technology:

The use of technologies, tools and infrastructure to promote and reinforce safe practise. As a minimum schools should:

- ✓ Identify all technologies and risk assess them
- ✓ Consider the use of additional software and/or settings for technologies to limit the risk
- ✓ Use up to date security software/solutions
- ✓ Use web content filtering product or service which must, as a minimum:

i. Subscribe to the Internet Watch Foundation Child Abuse Images and content (CAIC) URL list ii. lock 100% of illegal material identified by the Internet Watch Foundation iii. Capable of blocking 90% of inappropriate content in each of the following categories:
Pornographic, adult, tasteless or offensive material
Violence (including weapons and bombs) Racist, extremist and hate material,
Illegal drug taking and promotion Criminal skills and software piracy

1.4.3 Education and training:

Ensure effective education to support digital citizenship and adapt delivery to address emerging risks. As a minimum schools should:

- ✓ Aim to raise awareness through education and training
- ✓ Incorporate eSafety in the school's training strategy e.g. safety awareness, acceptable use, safeguarding procedures
- ✓ Ensure the training strategy includes ongoing support for existing staff and induction training for new staff
- ✓ Make staff aware of local, regional and national issues related to esafety and ensure they are confident in their abilities to escalate an incident if necessary and/or appropriate
- ✓ Consider the role of the school in providing esafety information and guidance to parents and carers and others in the family unit

1.4.4 Standards:

Ensure procedures are in place to monitor and review practise and regular audits take place to monitor effectiveness. As a minimum schools should:

- ✓ Gathering information to establish the extent of current awareness and training materials available,
- ✓ Review and evaluate all internal policies and procedures (at least every 12 months or sooner if required by new technologies or esafety incident)

1.5 The importance of an acceptable use policy:

An acceptable use policy (AUP) provides a clear statement of the reasons why internet use is provided and the advantages. This includes the benefits of email systems, ability to get information from websites, connection to other people through email, social networking, instant messaging, webcasting, mobile phones and gaming etc. It sets out the roles, responsibilities and procedures for the acceptable, safe and

responsible use of all online technologies and also how the school will provide support and guidance to parents/carers, families and the wider community for the safe and responsible use of these technologies beyond the school setting. Schools provide access to the internet for the benefit of the school community; use of the facility should be regarded as a privilege and users should be clear that there are procedures for dealing with unacceptable behaviour or misuse. The object is to promote a culture of safety which is underpinned by clear expectations of responsible behaviour. Schools must ensure that they have an AUP that is appropriate to the user group (staff, pupils, governors and other stakeholders)

The most important part of an AUP is the code of conduct governing the behaviour of users when they are connected to the network. It must be clear that access to the facilities is a privilege and not a right and is provided dependent on the agreement to comply with the specified behaviours and that any breach of the policy could result in sanction. Obviously the sanctions will depend on the user (pupil, staff member, volunteer, governor etc.) and the nature of the misuse and could range from temporary withdrawal of the facility to reporting to the police if the action is illegal. It is appropriate to have different acceptable use policies to cater for the range of user groups.

The AUP should include a description of what is commonly referred to as "netiquette" a collective term for acceptable behaviour while online, for example, appropriate language, ensuring activities do not disturb or disrupt other users and that activities are not illegal. Unacceptable use may include creation and transmission of offensive, obscene or indecent documents or images, creation and transmission of material designed to cause annoyance, inconvenience or anxiety, creation of defamatory material, creation of content that infringes copyright. In some cases, inappropriate use may be use of the network to waste time, violate the privacy of others or use of software or applications which may put the network at risk.
It is good practise to include a disclaimer in an AUP to absolve the school from responsibility under specific circumstances. The AUP should also include a statement:

- that the AUP is in compliance with telecommunication rules and regulations
- regarding the need to maintain personal safety and privacy while on the network and online
- regarding the need to comply with copyright regulations

1.6 Roles and Responsibilities:

esafety is not a discreet role and cannot be assigned to a single member of staff. Effective esafety is achieved through a whole school approach however there are some responsibilities which sit with a specific role in the school.

1.6.1 The Headteacher:

- Takes overall responsibility for esafety provision.
- Takes overall responsibility for data and security provision (Senior Information Risk Owner).
- Ensure the school uses an approved, filtered internet service which complies with current statutory requirements.
- Is responsible for ensuring that staff receive suitable training to carry out their esafety roles and to train other colleagues as relevant.
- Is aware of the procedures to be followed in the event of a serious esafety incident.
- Review regular monitoring reports from the eSafety Co-ordinator.

- Ensures there is a system in place to monitor and support staff that carry out internal esafety procedures.

1.6.2 Governors and eSafety Governor

- Ensures the school follows all current esafety advice to keep the children and staff safe.
- Provides support to the governor with esafety responsibilities.
- Approves the esafety policy and review the effectiveness on an ongoing basis through regular reports to the governing body on any incidents and actions taken to address them.
- Supports the school in encouraging parents and the wider community to become engaged in esafety activities.

1.6.3 School Business Manager/Administrator:

- Ensures all personal and sensitive data held on office machines is appropriately protected through access controls (Information Asset Owner).
- Ensures that information held on office machines is done so in compliance with the Data Protection Act.

1.6.4 Network Manager/Technician:

NB: If the school does not employ a Network Manager/Technician, the roles and responsibilities detailed here must be considered by Headteacher and allocated to an officer/provider who is clear about the requirement and sufficiently skilled and knowledgeable to undertake the duties.

- Ensures the security of the school ICT system and keep up to date documentation of the school security and technical procedures.
- Ensure users can only access the school network through an authorised and properly enforced password protection policy.
- Ensures the school network benefits from protection again misuse and malicious attacks.
- Web filtering is applied and updated on a regular basis.
- Ensures access controls and encryption is in place to protect personal and sensitive information held on school owned devices.
- Ensures appropriate backup procedures exist so that business critical information can be recovered in the event of an emergency.
- Reports any actual or attempted misuse for investigation.
- Keeps up to date with the school safety policy and updates others as relevant.

1.6.5 School eSafety Co-ordinator; Miss M Whitby

Designated Child Protection Lead: Mr S Watson

- Has day to day responsibility for esafety issues and leading role in the implementation and review of esafety policies and practises.
- Is up to date on esafety issues and legislation.
- Promotes awareness and commitment to esafety throughout the school.
- Liaises with school ICT technical staff/providers.

- Communicates regularly with SLT and the designated eSafety Governor/committee to discuss issues, review incident logs and filtering and change control logs.
- Ensures all staff are aware of the procedures that need to be followed in the event of an esafety incident and that an esafety log is in place and maintained.
- Facilitates training and provides advice.
- Liaises with the Local Authority and relevant agencies.

1.6.6 Computing Curriculum Lead:

- Oversees the delivery of the esafety element of the computing curriculum.
- Liaises with the esafety co-ordinator regularly.

1.6.7 All Staff:

- Read, understand and promote the school esafety policy and procedures.
- Sign and adhere to the school staff Acceptable Use Agreement.
- Demonstrate safe and responsible behaviours in their own use of technology.
- Be aware of esafety issues and potential risks including those related to the use of mobile phones, camera and other mobile devices. Ensure school policies are adhered to.
- Ensure digital communications with pupils are on a professional level and through school based systems only.
- Report suspected misuse or problems to the esafety co-ordinator or responsible lead in their absence.

1.6.8 Teachers:

- Embed esafety awareness raising in all aspects of the curriculum and other school activities.
- Supervise pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities as relevant).
- Inform pupils about the use of the internet for research and ensure they are aware of legal issues relating to electronic content including but not exclusively copyright law.
- Understand and comply with the school policy on the use of phones, cameras and other mobile devices.
- Understand and comply with the school policy on the use of photographic images.
- Understand the importance of adopting good safety practise when using technology outside school and that the school esafety policy covers their actions out of school (if related to their membership of the school).

1.6.9 Pupils:

- Take responsibility for learning about the benefits and risks of using the internet in school and outside.
- Read, promote and adhere to the Pupil Acceptable Use Agreement.
- Understand the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Understands what to do if they or someone they know feels worried or vulnerable when using online technology.

- Understand and comply with the school policy on the use of phones, cameras and other mobile devices.
- Understand and comply with the school policy on the use of photographic images and on cyber-bullying.
- Understand the importance of adopting good esafety practise when using technology outside school and that the school esafety policy covers their actions out of school (if related to their membership of the school).

1.6.10 Parents/Carers:

- Support the school in promoting esafety and endorse the Parent Acceptable Use Agreement.
- Support and promote the Pupil Acceptable Use Agreement with their children.
- When accessing information through the school online facilities, do so in accordance with the Parent Acceptable Use Agreement.
- Notify the school if they have any concern about their child/children's use of technology.

1.6.11 External groups:

- Any external individual or representative of an organisation will sign an acceptable use agreement before using any equipment or internet in the school.

1.7 Communication of this policy:

- This policy will be posted on the school website, will be available in the staffroom and classrooms and other areas where resources are shared.
- This policy will be part of the school induction pack for new staff and will be included in the staff handbook.
- Acceptable use agreements to be signed by all staff, governors and other members of the school community.
- Acceptable use agreements to be discussed with pupils at the start of each academic year.
- Signed acceptable use agreements will be held on pupil and staff files.

1.8 Handling complaints:

The school will take all reasonable precautions to ensure esafety but the rapid changes and expansion of technologies and content make it impossible to guarantee that inappropriate content will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed or any consequences thereof.

Staff, pupils and other members of our school community have been made aware of this policy and are aware of potential implications of any infringement.

Complaints concerning cyberbullying are dealt with in accordance with our Antibullying Policy. Complaints related to child protection are dealt with in accordance with our School and Local Authority child protection procedures

1.9 Review and monitoring of this policy:

This esafety policy has been reviewed by our school senior leadership team and is current and appropriate for its intended purpose and audience. It has been approved for adoption by the School Governing Body and has been communicated across the school community. The policy will be reviewed annually or earlier if there are significant changes to technologies or how they are used; any changes will be notified to the school community as they occur.

This esafety policy will be referenced in other school policies including (but not exclusively): ICT and Computing Policy, Behaviour Policy, Child Protection Policy, AntiBullying Policy, Behaviour Policy, Data Protection Policy and the School Development Plan.
The school safety co-ordinator is responsible for the document ownership, review and updates.

2.0 Education and curriculum:

Our school has and an education programme which covers a range of skills and behaviours appropriate to role, age and experience with the objective of supporting everyone to model safe and responsible behaviour in the use of technology. This education programme includes:

2.1 Pupil e-safety curriculum:

We will teach pupils:

- ✓ How to understand acceptable behaviour in an online environment: to be polite and not use abusive/bad/inappropriate language or other behaviour.
- ✓ How to develop a range of strategies to evaluate and verify information before accepting its accuracy.
- ✓ To be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what this might be ✓ To know how to narrow down or refine a search.
- ✓ [For older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- ✓ To understand how photographs can be manipulated and how online content can attract the wrong sort of attention.
- ✓ To understand why "online friends" may not be who they say they are and why they need to be careful.
- ✓ To know to keep personal information private and understand why they should not post or share details accounts of their personal lives, contact information, daily routines, locations, photographs and videos.
- ✓ To know how to ensure they have turned on privacy settings.
- ✓ To understand why they must not post pictures or videos of others without their permission.
- ✓ To know not to download any files – such as music files – without permission.
- ✓ To have strategies for dealing with receipt of inappropriate materials or things that upset them.
- ✓ [For older pupils] to understand why and how some people will "groom" young people for sexual reasons.

- ✓ To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- ✓ To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies i.e. a parent or carer, teacher or trusted staff member, an organisation such as Childline or by clicking the CEOP button. ✓ To be good digital citizens.
- ✓ To understand their digital footprint and its importance. ✓ To STOP and THINK before they CLICK.

In addition, the school:

- Plans internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

- Reminds pupils of their responsibilities through an Acceptable Use Policy which they sign. The Acceptable Use Policy is also displayed throughout the school.

2.2 Staff and pupils:

Our school:

- ✓ Ensures staff model safe and responsible behaviour in their own use of technology.

- ✓ Ensures that staff and pupils understand the issues of plagiarism and copyright when using materials sourced from the internet. Staff and pupils know that they must respect and acknowledge copyright and intellectual property rights.

- ✓ Ensures that staff and pupils understand the issues around the commercial use of the internet including risks in pop-ups, purchasing online, online gaming and gambling.

2.3 Staff and governor training:

Our school:

- ✓ Ensures staff know how to send or receive sensitive and personal data and understands when and how to apply additional security.

- ✓ Makes training available to staff on esafety issues, including information security and data protection.

- ✓ Provides all new staff, including those on placement and work experience, with information and guidance on the esafety policy and the acceptable use policy.

- ✓ Ensures our governing body reviews our policies at least annually (or more frequently if there are significant changes) and is provided with opportunities to engage in training rolled out across the school.

2.4 Parent/Carer awareness and training:

Our school has a rolling programme of advice, guidance, training and support for parents and carers which includes:

- ✓ Acceptable Use Agreements to ensure the principals of appropriate and responsible online behaviour are made clear to parents and carers.
- ✓ Information through leaflets, school newsletters and the school website.
- ✓ Awareness raising sessions at the school.
- ✓ Suggestions for safe internet use at home.
- ✓ Information about national support sites and how to get help.

3.0 Expected conduct and incident management:

3.1 All users:

- Are responsible for using the school ICT systems in accordance with the acceptable use policy (and any other policies which govern access to the applications) which they will be expected to sign before being given access to school systems. In some circumstances it will be appropriate for parents/carers to sign on behalf of pupils.
- Need to understand the importance of misuse or access to inappropriate materials and be aware of the potential consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to report any such incidents.
- Should understand the importance of adopting good esafety practise when using digital technologies out of school and realise that the school's esafety policy covers their actions out of school if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and other mobile devices. They should also know and understand the school policy on taking/use of images and on cyberbullying.

3.2 Staff and governors:

- Are responsible for reading and making sure they understand the school esafety policy and acceptable use policy and using the ICT systems accordingly. This includes the use of mobile phones and hand held devices.

3.3 Pupils:

- Should read and act in accordance with the school acceptable use policy.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.4 Parents/Carers:

- Should provide consent for pupils to use the internet (and other relevant/appropriate technologies) as part of the esafety acceptable use agreement at the time of their child's entry to the school.
- Should know and understand the rules of appropriate use and the potential for sanctions if there is misuse.

3.5 In our school:

- There is strict management, monitoring and application of the esafety policy and a differentiated and appropriate range of sanctions although we appreciate that the behaviour of users is generally positive and there is rarely a need to apply sanctions.
- All members of the school community are encouraged to be vigilant in reporting issues and are confident that issues will be dealt with quickly and sensitively.
- Support is actively sought from other agencies as needed to deal with esafety issues.
- Esafety incidents are reported and monitored – this contributes to the further development of policies and practise. Any reports are reviewed/audited and reported to the school senior leaders, governors, Local Authority and LSCB as required.
- Parents/carers are informed of esafety incidents involving young people for whom they are responsible. We communicate with senior leaders of other schools as required.
- We will contact the Police if one of our staff or pupils receives an online communication that we consider to be particularly disturbing or breaks the law.

4.0 Managing the ICT Infrastructure:

4.1 Internet access, security (virus protection) and filtering:

Our school:

- ✓ Has filtered secure broadband connectivity provided through the Council's CIN agreement.
- ✓ Uses internet filtering system which blocks sites by categories including (but not exclusively) pornography, race hatred, gaming, sites of an illegal nature. Our filtering solution provides user level filtering where relevant, closing down or opening up options as appropriate to the age/key stage of the pupils.
- ✓ Has anti-virus software provided as part of the Council's CIN agreement and the network is set up so staff and pupils cannot download executable files.
- ✓ Uses DfE and/or Local Authority approved email systems.
- ✓ Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform.
- ✓ Only unblocks other external social networking sites for specific purposes and records when this has been the case and the reason.
- ✓ Has blocked pupil access to music downloads or shopping sites – except those approved for educational purposes at regional or national level.

- ✓ Works with the School Information and Technologies Strategic Board to ensure any concerns about the system are communicated to ensure the systems remain robust and protect users.

- ✓ Is vigilant and robust (in so far as it is practicable and reasonable) in its supervision of pupils.

- ✓ Ensures all staff and students have signed the acceptable use agreement and understands that they must report any concerns.

- ✓ Ensures pupils only publish within an appropriately secure environment

- ✓ Requires staff to preview websites before use (where they have not been previously viewed or cached) and signpost pupils to age and subject appropriate websites.

- ✓ Plans the curriculum context for internet use to match pupil age and ability.

- ✓ Encourages the use of child friendly search engines where open internet searching is required, e.g. yahoo for kids, ask for kids or Google Safe Search.

- ✓ Does not allow or is vigilant when conducting "raw" image search with pupils e.g. Google Image Search.

- ✓ Informs all users that internet use is monitored.

- ✓ Informs staff and pupils that they must report and incident or failure of the filtering system immediately and must log the details and track to resolution, escalating if necessary.

- ✓ Ensures that all users are aware of and understand the rules of appropriate use and the sanctions that may result from misuse.

- ✓ Provides advice and information to all members of the school community on how to report offensive materials, abuse and bullying.

- ✓ Reports any material suspected to be illegal to the appropriate authorities.

4.2 Network Management (user access, backup)

Our school:

- ✓ Uses individual, audited logins for all users.

- ✓ Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.

- ✓ Ensures the System Administrator/Network Manager (or the designated lead as identified by the Head Teacher) is up to date with services and policies and requires the technical support provider to be up to date with services and policies.

Storage of all data within the school conforms with the requirements of the Data Protection Act including the requirement for data stored online to conform to the EU Data Protection Directive where storage is hosted within the European Union.

- ✓ Ensures our technical provider is aware of and compliant with the KMBC Network Standards.

To ensure the network is used safely, this school:

- ✓ Ensures staff read and sign that they have understood the school safety policy and are provided with network, internet and email access on this basis.

- ✓ All pupils have their own unique username and password which gives them access to the network and the internet.

- ✓ Makes it clear that passwords should never be shared and users must always log on with their own credentials.

- ✓ Has set up the network with a shared area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.

- ✓ Requires all users to log off when they have finished working or are leaving the computer unattended.

- ✓ If a user finds a logged on machine, they are required to log off and then log on again as themselves. Staff machines are timed out after ten minutes and users will have to re-enter their credentials to continue working.

- ✓ Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again or have crashed. Computers should be turned off at the end of the day.

- ✓ Has set up the network so that users cannot download executable files/programmes.

- ✓ Has blocked access to music/media download or shopping sites – except where approved for educational purposes.

- ✓ Scans all mobile equipment with anti-virus/spyware before it is connected to the network.

- ✓ Makes clear that staff are responsible for ensuring that any computer or laptop on loan to them from the school is used solely for their professional responsibilities

and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- ✓ Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained to ensure the protection of the device and the school network.

- ✓ Makes clear that staff accessing Local Authority systems do so in accordance with the relevant corporate policies.

- ✓ Maintains equipment to ensure the health and safety of its employees.

- ✓ Ensures that access to the school network resources by staff from remote locations is restricted to a needs only basis and is accessed only through approved systems.

- ✓ Does not allow any outside agencies to access our network remotely except where there is a specific professional need. In these cases access is restricted, is only through approved systems and is covered by appropriate data processing agreements. Examples of such circumstances may be technical support on SIMS, Education Welfare Officers accessing attendance data on specific children, parents/carers using a secure portal to access information on their child – in all cases the access must be restricted to authorised people

- ✓ Has a clear disaster recovery system in place for business critical data that includes a remote back up of critical information (in compliance with audit requirements).

- ✓ Uses our broadband network for our CCTV system and have had set up approved partners. A CCTV Policy is in place and the operation of the CCTV system is compliant with the requirements of the Data Protection Act.

- ✓ Uses the DfES secure s2s website for all CTF files sent to other schools.

- ✓ Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our Local Authority.

- ✓ Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.

- ✓ Our wireless network has been secured to industry standard Enterprise security level/appropriate standards for educational use.

- ✓ Projectors are maintained to ensure the quality of the presentation remains high.

- ✓ All computer equipment is installed professionally and meets health and safety standards and is reviewed regularly to ensure continued compliance with safety requirements.

- ✓ Ensures that our technical support provider/s are aware of the parts of this policy that apply to them and are in compliance.

4.3 School Management Information System:

- ✓ Access to the school management information system is controlled through a separate password for data security purposes.

- ✓ Access to the school management information system is configured to ensure that users can only access modules required to perform their role.

- ✓ Is clear about the responsibilities for the daily back up of MIS and finance systems and other significant business information. In the case of SIMS and centralised storage, this is managed through the Council's IT Service.

- ✓ Our school has a Data Protection Policy which includes a requirement for staff to be trained in their responsibilities under the Data Protection Act.

4.4 Password policy:

- ✓ Our school makes it clear that members of our school community must always keep their password private, must not share it and must never leave it where others can find it.

- ✓ All staff have their own unique username and password to access systems – they are responsible for keeping their password private.

- ✓ We require staff to use strong/complex passwords for access to our MIS system.

- ✓ Staff are prompted to change their password every 30 days.

4.5 Email:

Our school provides staff with an approved email account for their professional use and makes it clear that personal email should be sent through a separate account. We do not publish email addresses of staff or pupils on the school website and use anonymised email accounts for communication with the wider public.

We will consult with the Local Authority and if necessary contact the Police if any of our staff or pupils receives an email that we consider to be particularly disturbing or breaks the law. We will also report messages that appear to support illegal activities to the relevant authorities and if necessary to the Police.

We ensure that ensure that email accounts are maintained and up to date and use technologies to protect users and systems against SPAM, phishing and viruses.

4.5.1 Pupils:

- ✓ Pupils are introduced to and use email as part of the ICT computing scheme of work.

- ✓ Reception and Y1 pupils are introduced to the principles of email through closed "simulation" software.

- ✓ Pupils can only receive external mail from and send external mail to addresses if the rules have been set to allow this for a specific curriculum requirement.

- ✓ Pupils are taught about the safety and "netiquette" of using email both in school and at home.

Specifically, they are taught:

- Not to give their email address unless it is part of a school managed project or to someone they know and trust and it is approved by their teacher or parent/carer.

- That email is a form of publishing where the message should be clear, short and concise.

- That any email sent to an external organisation should be carefully written and authorised before sending in the same way as a letter written on school headed paper.

- They must not reveal private details of themselves or others in email such as address, telephone number etc.

- That embedding adverts or forwarding "chain" emails is not allowed.

- That they should think very carefully before sending any attachments and should not open attachments unless they know the source is safe.

- That they must immediately tell a teacher or responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying.

- Not to respond to malicious or threatening emails, but to keep them as evidence.

- Not to arrange to meet anyone they meet through email without having discussed with an adult or taking a responsible adult with them.

- To "Stop and Think Before They Click".

- ✓ Pupils sign the school acceptable use agreement to say they have read and understood the esafety rules which include the use of email and we explain how any inappropriate use will be deal with**.**

4.5.2 Staff:

- ✓ Staff are provided with an approved email system and know that this is the only email to be used for business purposes. Personal email addresses must not shared with pupils or their parents/carers.

- ✓ Know they need to be particularly careful if they are required to send staff or pupil personal information. Secure systems such as S2S (for school to school transfer) or Collect should be

used where possible. Further information is provided in the Information and Data Security Policy for Schools.

- ✓ Know that emails sent outside the school must be written carefully (and in some instances may require approval) in the same way as a letter written on school headed paper and emails should follow the school 'house style'.

- ✓ Know that the sending of multiple or large attachments should be limited and may be restricted.

- ✓ Know the sending of chain letters and embedded adverts is not allowed.

All staff sign our school acceptable use agreement to say they have read and understood the esafety rules, including email and we explain how any inappropriate use will be dealt with.

4.6 School website:

- ✓ The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of the presentation is maintained.

- ✓ Uploading of information is restricted to our website administrator.

- ✓ The school website complies with the Statutory DFE Guidelines for Publications.

- ✓ Most of the material published on the website is the schools' own work but where other work is published or linked to we credit the sources used.

- ✓ The point of contact on the website is the school address and telephone number. We use a general email contact address e.g. stmariescps.org.uk. Individual email identities will not be published.

- ✓ Photographs published on the website do not have full names attached.

- ✓ We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

- ✓ We do not use embedded geo data in respect of stored images.

- ✓ We expect teachers using school approved blogs or wikis to password protect them and run them from the school website.

4.7 Social networking:

Teachers must not run social network spaces for student use on a personal basis or to open up their own spaces to their pupils. The schools' preferred system for communication with pupils must be used.

The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students, pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.
- Parents. carers and pupils must not use social media to raise concerns or complaints – these should always be raised with the school directly.

4.8 Video Chatting (including Skype and other online video chat applications):

Our school:

- ✓ Only uses approved or checked webcam sites.
- ✓ Informs parents/carers that video chat, recording and streaming with other schools or external organisations is being used by the school.
- ✓ Ensures that pupils do not use video chat equipment without supervision by a teacher or appropriate adult.
- ✓ Ensures that when video chat equipment or software is not in use it is deactivated or the camera lens is covered in case it reconnects unexpectedly.

4.9 CCTV & filming:

4.9.1 We have CCTV in our school for the prevention and detection of crime. Although the ICO does not regulate the use of CCTV it does produce guidance and in compliance with this the school registration includes notification of the CCTV system. Careful consideration has been given to the location of cameras and how long records are kept. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation. We have a CCTV Policy in place.

4.9.2 We use recording equipment on occasions as a tool to capture and share best teaching practise. We do not release these recordings outside of the school staff and will not use them for any other purposes.

Filming for curriculum purposes should have a specific purpose and outcome. In all cases, appropriate consent should be in place.

Further information is available in the Information and Data Security Guidance for Schools.

5.0 Information and data security

Our school has an Information and Data Security Policy which details the specific measures in place to protect the information entrusted to the school for the performance of its duties. We also have a Data Protection Policy which has been issued to all staff. All staff are DBS checked and with a record kept in a single, central record. Staff know:

- ✓ That the Headteacher is the Senior Information Risk Owner (SIRO).
- ✓ Who the key contacts for school information (Information Asset Owners) are. We have a register of information and the responsible Information Asset Owners.
- ✓ That technical measures are in place to protect information and that they must not take any action that may compromise the effectiveness of these measures.
- ✓ They must report any incidents where information has or may have been compromised.

We ensure all stakeholders (staff, pupils and governors) sign an acceptable use agreement (which is clear about responsibilities relating to data security, passwords and access) and we have a record of who has signed.

We follow local authority guidelines for the transfer of data (such as MIS data or reports on children) to professionals working in the local authority or their partners in children's services, health, welfare and social services.

We require that any protected or restricted material must be encrypted if the material is to be removed from the school and we limit any such data removal. We have a data protection policy which is specific about the requirement to protect personal and sensitive information.

Staff with access to setting up usernames and passwords for email, network access and learning platforms are working within the approved system and follow the security processes required by those systems.
We apply a records retention policy and we ask staff to undertake housekeeping, at least annually, to review, remove and destroy any digital materials and documents that no longer need to be stored.

5.1 Transferring information:

Staff devices are encrypted with a centrally managed solution provided under the Council's CIN agreement or benefit from an industry standard, locally managed encryption solution

Staff have access to approved email systems for business use.

Staff have secure areas on the school network to store sensitive documents or photographs.

We require staff to logout of systems when leaving their computer but also enforce lock out after 10 minutes.

We only use encrypted devices (including flash drives/removable media) if a member of staff has to take any personal information off site.

We use the DfE S2S site to securely transfer CTF pupil data files to other schools.

We store hard copy personal information in locked storage cabinets in a lockable area.

5.2 Server management:

Servers are located in lockable areas and managed by staff with DBS clearance.

Our systems are backed up to a remote location – no back-up tapes leave site.

We use Knowsley Council's virtualised server infrastructure for disaster recovery on our network/admin/curriculum servers.

We ensure our technical provider/s are aware of this policy and are in compliance with the elements that that apply to them.

5.3 Asset management and disposal:

In our school:

Details of all school owned hardware assets are recorded in an inventory and we keep a record of who has the asset at any given point in time.

Details of all school owned software assets are recorded in an inventory.

We comply with the Waste Electrical and Electronic Equipment Directive 2013 on equipment disposal by using an authorised, approved or recommended disposal company for disposal of equipment where any personal data may have been held. In these cases the storage media will be forensically wiped and the school will obtain a written guarantee that this will happen. If the storage media has failed it will be physically destroyed. In all cases, a certificate of destruction will be obtained and held with the asset register.

Portable equipment loaned by the school is disposed of in the same manner.

We are using secure file deletion software/wiping devices thoroughly.

Paper based sensitive information is shredded using a cross cut shredder and/or collected by a secure data disposal service.

6.0 Use of personally owned mobile devices including mobile phones:

The use of mobile technologies is now inherent in the way most people live their lives and because of the functionalities available through devices and improvements in network connectivity and affordability, these devices have become essential pieces of equipment. There has been a rapid expansion in the number of people who now use tablet devices in addition to or as a replacement for mobile phones. In addition to measures in place related to school owned devices, the school has procedures in place to govern the use of personally owned equipment including mobile phones, table devices and cameras. Personally owned devices are those which have not been provided by the school for connection to the school's primary network. These procedures govern the functionalities irrespective of the device they are available on.

6.1 Pupil use of personal devices including mobile phones:

- Our school strongly advises that pupils should not bring their mobile phones into school/ or no pupils should bring their mobile phone or personally owned mobile device into the school and any such devices brought into the school will be confiscated. Mobile phones and other mobile devices brought into school are done so entirely at the owners' own risk. Our school accepts no responsibility for the loss, theft or damage of any phone or mobile device brought into the school.
- If a pupil needs to contact their parent/carer they will be allowed to use a school phone.

- The school accepts that there may be particular circumstances in which a parent/carer wants their child to have a mobile phone for safety. If permission is given by the school, pupil mobile phones which are brought into the school must be turned off (not put on silent) and stored out of sight on arrival at school. Parents are advised not to contact their child via their mobile phone during the school day but to contact the school office instead.
- Pupils will be instructed in the safe and appropriate use of mobile phones and mobile devices and will be made aware of boundaries and consequences.
- If a pupil breaches school policy the phone or device will be confiscated and will be held securely in the school office. Mobile phones and devices will be released to parents/carers in accordance with school policy.
- Pupils should protect their information by only giving their phone number to trusted friends and family members.
- Phones and mobile devices must not be taken into examinations. Pupils found in possession of a mobile phone during an examination will be reported to the appropriate examination body which may result in their withdrawal from either that or all examinations.
- Pupils may be issued with mobile phones/hand held devices to use in specific learning activities under the supervision of a member of staff. These devices will be set up so that only those features required for the activity will be enabled.
- If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity it will only take place when approved by a member of the senior leadership team.

6.2 Staff use of personal devices including mobile phones:

- Mobile phones and other mobile devices brought into school are done so entirely at the owners' own risk. Our school accepts no responsibility for the loss, theft or damage of any phone or mobile device brought into the school.
- All mobile phone use is open to scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time if it is deemed to be necessary.
- Mobile phones and personally owned devices will be switched off or switched to "silent" mode. Bluetooth communication should be "hidden" or switched off.
- Mobile phones and personally owned devices will not be used during lessons or formal school time unless permission has been granted by a member of the senior leadership team for an emergency circumstance – they should be switched off or silent at all times. Staff may use their mobile devices during break times. If a staff member is expecting a personal call they can leave their phone with the school office to answer on their behalf or ask permission to use the phone other than at break times.
- Staff should not use personally owned devices, including mobile phones or cameras, to take photographs or videos of pupils and will only use work provided equipment for this purpose. In exceptional cases the Headteacher may give permission for personally owned devices to be used and in such cases the images must be transferred to the school network as soon as is practically possible and the media deleted from the device.
- No images or videos should be taken without the prior consent of the person or people concerned and that consent is informed and appropriate.
- Mobile phones and personally owned devices are not permitted in certain areas within the school site including changing rooms, toilets and in some settings bathrooms, sleep and changing areas.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside the school in professional capacity. Staff will be given access to a school phone where contact with pupils or their family is required.
- Where a member of staff is required to use a mobile phone for school duties, for instance in the case of an emergency during off site activities or for contacting students or parents, a mobile phone will be provided and used. In an emergency where the member of staff doesn't have access to a school owned device, they should use their own device and hide their own mobile number for confidentiality purposes. Guidance on how to do this is included in the useful links section.
- Staff mobile phones and other mobile devices may be searched at any time as part of routine monitoring.

6.3 Other school stakeholders:

- Mobile phones and other mobile devices brought into school are done so entirely at the owners' own risk. Our school accepts no responsibility for the loss, theft or damage of any phone or mobile device brought into the school.
- All visitors are required to keep their phones on silent.
- Bluetooth or similar functions on a mobile phone should be switched off at all times and not used to send images or files to other mobile phones.
- Our school reserves the right to search the content of any mobile device on the school premises where there is a reasonable suspicion that it may contain undesirable material including (but not exclusively) pornography, violence or bullying.

7.0 Digital images and video:

In our school:

- ✓ We get parent/carer permission for the use of digital photographs or video involving their child/children as part of the school agreement form.
- ✓ We do not identify pupils in online photographic materials or include the full names of the pupils in the credits of any published school produced video materials, on DVDs or in image filenames.
- ✓ Our Staff Acceptable Use Policy includes a clause on the use of mobile phones or other personally owned mobile equipment for taking photographs of pupils.
- ✓ We obtain individual parent/carer or pupil permission (prior to publication) for long term use before individual pupil photographs (not group photographs) are used on the school website, in the school prospectus or in other high profile publications.
- ✓ We block/filter access to social networking sites or newsgroups unless there is a specific educational purpose.
- ✓ We teach children to consider how to publish for wide range of audiences which might include their parents/carers, younger children, the school governor and the wider community as part of their ICT scheme of work.
- ✓ We teach pupils that they should be very careful about posting personal photographs on online network spaces and they are also taught how images posted online can be manipulated to cause upset. They are also taught to understand the need to maintain privacy settings to keep their personal information safe.
- ✓ We teach pupils that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with

their images (including the name of the file) that reveals the identity of others and their location such as house number, street name or school. We teach them about the need to keep their information secure.

- ✓ We teach pupils about the need to respect themselves and other people in their online behaviour and tell them how to report bullying or abuse and what to do if they are worried.

8.0 Concluding statement:

When considering the safety of children and young people online, there is clearly a technological dimension. Service providers have a significant role but finding, reporting and taking down content doesn't get to the root of the problem. Mobile phone operators have now agreed to put content filters onto mobile phones automatically and proof of age (over 18) is required to deactivate them. Family friendly filters are in place across public Wi-Fi in areas where children are likely to be present (but children could be present almost anywhere). Google and Microsoft (which account for 95% of internet search traffic) now use software that means over 100,000 search terms will return no results and trigger warnings about the potential illegality of the searched for images. All internet service providers have rewired their technology so that filters, once installed, will cover any device connected to the home internet account. The default position for filters is now "on". These are positive actions but can only be effective as part of a holistic approach. A child in the Bryron Review, "Safe Children in a Digital World" summed this up:

"Kids don't need protection they need guidance. If you protect us you make us weaker. We don't go through all the trial and necessary to learn how to survive on our own … don't fight our battles for us – give us assistance when we need it."

Ref: Bryon Review: Safer Children in a Digital World, 2008

We need to help children to become responsible digital citizens and to do this families, industry, government, schools and other stakeholders need to work together not only to reduce the availability of potentially harmful material and restrict access to it but to develop resilience of children. Bryon says:

"It is about preserving their right to take the risks that form an inherent part of their development by enabling them to play video games and surf the net in a safe and informed way."

Ref: Bryon Review: Safer Children in a Digital World, 2008

As a school we are committed to this objective and have appropriate processes in place to support us in doing so.