St. Margaret Mary's Catholic Junior School

Pilch Lane
Liverpool
L14 0JG

E Safety and Acceptable Use of IT Policy

Committee to approve/ratify policy	Curriculum & Policies
Policy Co-ordinator	R Culley
Date of approval/ratification by Committee	September 2026
Date for renewal	September 2027
Signature of the Chair of the Committee	

Mission Statement:

Loving, learning, growing together with Jesus

St Margaret Mary's Catholic Junior School E-Safety Policy

Version Control Record:

Date: **January 2016**

Version: **2.0**

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

St Margaret Mary's Catholic Junior School eSafety Policy

Contents

Section	Subject	Page Number
	Table of contents	2
	Glossary	4
	Organisations	5
	List of appendices, references and useful links	7
1.0	**Introduction and overview**	9
	1.1.0 What are the risks?	9
	1.2.0 What is eSafety?	10
	1.3.0 Scope of the policy and the legislation	11
	1.3.1 Ofsted	11
	1.4.0 Strategic approach: BECTA PIES Model	12
	1.4.1 Policies and practises	12
	1.4.2 Infrastructure and technology	13
	1.4.3 Education and training	13
	1.4.4 Standards	14
	1.5.0 The importance of an acceptable use policy	14
	1.6.0 Roles and responsibilities	15
	1.6.1 The Headteacher	15
	1.6.2 Governors and eSafety Governor	15
	1.6.3 School Business Manager/Administrator	15
	1.6.4 Network Manager/Technician	15
	1.6.5 School eSafety Co-ordinator and/or Designated Child Protection Lead	16
	1.6.6 Computing Curriculum Lead	16
	1.6.7 All Staff	16
	1.6.8 Teachers	17
	1.6.9 Pupils	17
	1.6.10 Parents/Carers	17
	1.6.11 External Groups	18
	1.7.0 Communications Strategy	18
	1.8.0 Handling complaints	18
	1.9.0 Review and monitoring	18
2.0	**Education and Curriculum**	19
	2.1 Pupil e safety curriculum	19
	2.2 Staff and pupils	20
	2.3 Staff and governor training	19
	2.4 Parent/Carer awareness raising and training	20
3.0	**Expected Conduct and Incident Management**	21
	3.1 All users	21
	3.2 Staff and governors	21
	3.3 Pupils	21
	3.4 Parents and carers	21

	3.5 In our school …	22
4.0	**Managing the ICT Infrastructure**	22
	4.1.0 Internet access, security and filtering	22
	4.2.0 Network management (user access, backup, curriculum and admin)	23
	4.3.0 Management Information System	26
	4.4.0 Password policy	26
	4.5.0 Email	26
	4.5.1 Pupils	26
	4.5.2 Staff	27
	4.6.0 School website	28
	4.7.0 Social networking	28
	4.8.0 Video chat (including SKYPE and other applications)	29
	4.9.0 CCTV and filming	29
	4.9.1 CCTV	29
	4.9.2 Other filming	29
5.0	**Information and Data Security**	30
	5.1 Transferring information	30
	5.2 Server management	31
	5.3 Asset management and disposal	31
6.0	**Use of personally owned devices including mobile phones**	32
	6.1 Pupil use of personal devices (including mobile phones/smart watches)	32
	6.2 Staff use of personal devices (including mobile phones/smart watches)	33
	6.3 Other stakeholders use of personal devices (including mobile phones/smart watches)	33
7.0	**Digital images and video**	34
8.0	**Concluding statement**	35

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 where 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/smart watches 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, smart watches, 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 (self-generated 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.

List of Appendices and References

Appendix 1: Acceptable Use Policy - pupils	36
Appendix 2: Acceptable Use Policy – staff and other stakeholders	39
Appendix 3: Social Media Policy – staff and other stakeholders	42
Appendix 4: Social Media Policy - pupils	45
Appendix 5: Protocol for responding to esafety incidents	49
Appendix 6: School IT Business Continuity Plan	50
Appendix 7: DfE Guidance – Copyright Licencing	54

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 pro-anorexia, 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 well-being (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:

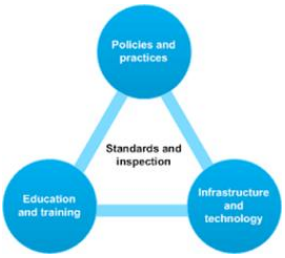
From September 2014 Ofsted significantly reduced the amount of guidance it publishes for inspectors, schools and other stakeholders. As of January 2015, there are three guidance documents:

- 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 practices:

Safer management through effective policies, procedures and practices - as a minimum school 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 school 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 school 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, smart watches 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:

- 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/Designated Child Protection Lead:

- 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, smart watches, camera's 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 e safety 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, smart watches, 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, smart watches 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 Anti-bullying 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, Anti-Bullying 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, smart watches, 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, smart watches 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 Smoothwall

✓ 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 'Stones Computing' 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 3 months.

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 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.

- ✓ 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 be 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. info@schooladdress. 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 and smart watches:

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, smart watches, 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/smart watches:

- Our school strongly advises that pupils should only bring their mobile phones/smart watches into school when the family have agreed and signed the mobile device agreement. Without a pre-agreed contract in place 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/smart watch for safety. If permission is given by the school, pupil mobile phones/smart watches 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/smart watch 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/smart watch 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/smart watches:

- 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/smart watch 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, smart watches 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 smart watch 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/smart watch 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/smart watches on silent.
- Bluetooth or similar functions on a mobile phone/smart watch should be switched off at all times and not used to send images or files to other mobile phones/smart watches.
- 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/smart watches 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.

Appendix 1

ICT Acceptable Use Policy
Pupil

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn and may have serious consequences.

Equipment

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will only use my personal hand held / external devices (mobile phones/smart watch /in school if I have permission.
- I will never eat or drink by ICT equipment.

Security and Privacy

- I will always keep my password to myself and never use someone else's logon name or password.
- I will always get permission before revealing my home address, telephone number, school name or picture on the Internet.
- I know that other computer users should be respected and should not be harassed, harmed, offended or insulted.
- I will respect the security on the computers and not attempt to bypass or alter the settings.
- I understand that staff may review my files and communications to ensure that I am using the system responsibly.

Internet

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing or video broadcasting (for example YouTube), unless I have permission from a member of staff.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.

- I will not open any attachments to emails, unless I know and trust the person / organisation that sent the email due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use chat and social networking sites with permission and at the times that are allowed
- I will respect the work and ownership rights of people, including abiding by copyright laws.
- I know that people on the Internet are not always who they seem. I will always ask a parent/guardian or teacher to go with me if I need to meet someone who I only know from the Internet or via email.

Email

- I will be polite and appreciate that other users may have different views from my own. The use of strong language, swearing or aggressive behaviour is not allowed.
- I will only open attachments to emails if they come from someone I know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If I receive an email containing material of a violent, dangerous, racist or inappropriate content, I will always report this to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you fail to comply with this agreement we may refuse you access to the Internet and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

I have read the Acceptable Use Policy and understand my responsibility to comply with requirements set down within it.	
Full name:	
Relationship to School:	Pupil
Signature:	
Date:	

Appendix 2

ICT Acceptable Use Policy Agreement
Staff and Other Stakeholders

The school has provided computers for use by staff. The computers are provided and maintained for the benefit of all staff and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of students or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / own mobile devices at school.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use."
- I agree that my use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
- I understand that any hardware and software provided for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will always get permission before installing, attempting to install or storing programs of any type.
- I will only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- I will always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- I will never eat or drink by ICT equipment.

Security and Privacy

- I will ensure all documents, data etc., are printed, saved, accessed and deleted/shredded in accordance with the school's Information Security Policy.
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I will keep my password to myself and never use someone else's logon name or password.
- I will always be wary about revealing my home address, telephone number, school name or picture on the Internet.
- I know that other computer users should be respected and should not be harassed, harmed, offended or insulted.
- I will respect the security on the computers and not attempt to bypass or alter the settings.
- I understand that the Head Teacher may review my files and communications to ensure that I am using the system responsibly.

Internet

- I will access the Internet for school activities only.
- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this as soon as possible.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Head Teacher on their request.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the Head Teacher.
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my school or professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my school or professional role.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute.
- I will only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

Email

- I will only use the school's approved systems to communicate with students and will only do so for teaching and learning purposes.
- I will be polite and appreciate that other users might have different views from my own. The use of strong language, swearing or aggressive behaviour is not allowed.
- I will only open attachments to emails if they come from someone I know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If I receive an email containing material of a violent, dangerous, racist or inappropriate content, I will always report this to the Head Teacher.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you do not here adhere to this policy access to the internet may be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read the Acceptable Use Policy and understand my responsibility to comply with requirements set down within it.	
Full name:	
Relationship to School:	
Signature:	

Date:	

Appendix 3

Social Media Acceptable Use Policy

Staff And Other School Stakeholders

Context:

Social media and other online communication tools are important and powerful but the nature of the internet means that social networking sites can leave teachers and the school they work for vulnerable and open to criticism if they fail to observe some simple precautions. Every comment we make informs opinions about us as people and professionals. The public have a right to expect that we model appropriate behaviour at all times. Our school welcomes the benefits of social media and manages the potential risks through awareness raising, policies and procedures. This acceptable use policy (which has been written to support appropriate, safe and positive use of social technologies) underpins the requirements set out in the esafety policy and supports staff members of our school community in ensuring that responsible digital citizenship is a reality.

Using Social Media with Pupils and Within the Context of Learning:

Where adults wish to use social media as part of the teaching and learning process this must have clear education objectives and intended outcomes. Senior leadership/line managers must be kept informed of the planned activities. This supports transparency and helps the school to manage concerns and in some cases objections raised by parents. Key considerations are:

- Children must be old enough to use the social media site. The age restrictions vary, but most stipulate that the user must be 13.
- The privacy options are appropriate and applied.
- Comments are moderated prior to publishing and learners are aware that any content must reflect themselves and their school in a positive light.
- The service used is generally recognised as trusted and reliable.
- Parents/carers have been notified that social learning will be used in their child's teaching.
- Responsive reporting systems are in place.
- The educational value of the activity has been shared with colleagues, learners and parents/carers.
- There is a pastoral/disciplinary process in place in the event of an incident.

Staff should be aware of the supporting processes in place to ensure appropriate actions are taken quickly when incidents happen. This includes how the school can support staff if they are the target of malicious activity online.

A key benefit of social media for schools is the opportunity to communicate directly with parents and carers, and this immediacy can help ensure they have the right information at the right time. Where parents and carers are invited to comment on children's online work, guidance should be provided to ensure all comments are positive and supportive. Despite this, negative comments may be posted and learners should be provided with strategies to cope with this eventuality.

Personal Use of Social Media by Adults Who Work With Children and Young People:

Remember - nothing is private and nothing can be deleted. Whether you're an active user of Facebook or an occasional contributor to online discussions your comments, observations, images, videos, reflections lead people to form an opinion about you and can get you and the school into difficulties. You need to consider carefully what your online profile says about you.

When using social media, staff:

✓ Should make it clear that their comments are personal and not representative of the school.

✓ Should stay clear of rumours or topics that can be associated with 'public anger.

✓ Should be careful not to compliment or criticise products and services - this could be construed as a professional endorsement.

✓ Should consider adding a disclaimer to their social media sites to the effect that any views expressed are those of the individual and not their employer. Putting a disclaimer on a social media site does not excuse content or exonerate the site owner from responsibility and in some cases disciplinary action may result.

✓ A disclaimer is not an excuse to post any content you wish to make and does not exonerate you of responsibility.

✓ Should ensure that their online conduct complies with the staff code of conduct and must act in accordance with the relevant school policies including the ICT Policy, esafety policy and this guidance.

✓ Must use the schools approved communication methods. In the case of Facebook – the school has a Facebook account where interactions are controlled, monitored and in accordance with the esafety policy.

✓ Must be aware of their online profile. Friends and family members may post content that could be misconstrued or considered inappropriate. In these cases, the person who posted the content should be asked to remove it.

When using social media, staff:

× Should not add parents, carers or children as friends or personal contacts in any social media.

× Should not engage in any role/school related discussion online (outside of formal channels).

× Should not make derogatory remarks about their employer/colleagues/pupils or their families.

× Should not publish their age, home address or other information they would not want their pupils to know.

× Should not post content that could be considered defamatory, derogatory or in breach of copyright legislation.

× Must not share personal or confidential information about the school, its staff or pupils online. Examples of this kind of information are staff changes, terms of employment, procurement, business partnerships and personal information about colleagues and children. Information of this kind must never be shared on social media. Where there is a legitimate reason to share information the school business processes must be followed.

Parents and Carers:

Parents sometimes raise concerns about the progress of their child, behaviour concerns etc. via a Facebook wall or message board. In all cases, the appropriate communication processes publicised by the schools should be

used. These processes have been designed to support professional and confidential discussion and problem resolution.

Where parents and carers are invited to comment on children's online work, guidance should be provided to ensure all comments are positive and supportive. It is not acceptable for anyone to post negative comments about any child on social media and the school need to be careful to ensure they are not complicit in this occurring.

Final Note:

All school stakeholders are expected to model appropriate online behaviour and good judgement in content published online. The school may be monitoring social media and will take seriously any content that could have a negative implication for the school, its staff, the pupils or the community it serves.

I have read the school social media policy and understand my responsibility to comply with requirements set down within it.	
Full name:	
Relationship to School:	
Signature:	
Date:	

Appendix 4

Acceptable Use Policy

Social Media – Pupils

Context:

Social media and other online communication tools can be very useful tools for educational, recreational and personal use if used properly. If not used properly they can cause upset and harm to you and to others. Every comment we put online gives the people who read it an opinion of what we are like as people and we should always try to make sure that we give the best impression because this matters now and in the future. We should also respect other people and not do anything online that could upset them or cause them harm. The law says that your school has a responsibility to help you to stay safe even when you are not in school.

We do not want to stop you being creative online but we do want to help you understand that actions (even those online) have consequences. We expect you to be a good ambassador for your school at all times, including when you are online. This policy and the school ICT Acceptable Use Policy are designed to help you to be a good digital citizen but you are responsible for your behaviour.

Using Social Media in School:

- You must read, understand and sign the school's ICT Acceptable Use Policy. If you do not understand it you must ask a teacher for help.
- You must not use chat or social media sites in school unless you have permission and are allowed to do so.
- You must always follow the instructions given to you. If you are not sure, you must ask your teacher for advice.

Using Social Media Outside School:

Always

✓ Check you are old enough to use the social media site. Age restrictions vary, but most stipulate that you must be at least 13. This is to protect your personal information and to stop you seeing something that could upset you or may be hurtful or harmful. You should not enter incorrect or false information to join social media networks.

✓ Make sure the privacy options are appropriate and applied. If in doubt, ask someone who understands to help you get it right. Remember to check the privacy options often.

✓ Use passwords that are hard for other people to guess (use a mix of letters and numbers). Never share or reveal your passwords and change them regularly.

✓ Make sure you have anti-virus software installed and keep it up to date.

✓ Check a website is secure before you put private information on it – a padlock symbol or https should appear in front or after the web address in the browser.

✓ Always think carefully before opening an attachment or clicking on a link or attachment sent from someone you don't know – it could contain a virus.

✓ Always unplug your webcam, cover the lens or point it at a blank wall when it's not in use.

✓ Always think carefully about what you share online. Things like profile pictures can give strangers clues to where you live.

✓ Remember – actions have consequences. You should only post things that you are happy for other people to see. Make sure you send messages only to the people you want to see them.

✓ Think carefully before you post especially before posting pictures or videos – these may give strangers clues to where you live.

✓ Think carefully before forwarding something you receive or before altering or forwarding pictures posted by someone else.

✓ Remember – once you post it you can't get it back. Even if you delete the information from a site you have little control over where it may have already gone.

- ✓ Think before your post. It is important to keep some things about yourself, your family and your friends to yourself. Some information is private and should stay that way but nothing is private online.

- ✓ Be courteous online just as you would be in person and think carefully about the language you use on line. Politeness counts!

- ✓ Create a safe screen name – a good screen name won't reveal much about how old you are, your gender or where you live.

- ✓ Always be careful who you chat to online. Not everyone who contacts you is who they say they are and you should be very careful if you are contacted by someone you don't know. If someone you don't know adds you as a friend, ignore them and delete the request. Check and update your friends list regularly.

- ✓ Remember, not everything you read online is true! Information online may be written from a particular point of view or may be written to mislead you.

- ✓ Be careful when someone tries to get you to spend money online – don't be tempted and keep your information secret.

- ✓ Think carefully about talking about a problem online. Some websites are there to help you but you need to be careful. If in doubt, talk with an adult you can trust.

- ✓ Trust your instinct – if something doesn't feel right it probably isn't.

- ✓ Always tell a trusted adult if you feel uncomfortable or threatened by something that happens online.

- ✓ Remember that once an image is sent or posted, there is no getting it back. Once you send or post a picture online you lose control of who sees it and what happens to it.

Online bullying can make you feel embarrassed, scared or upset. It can seem like it will never end but there are things that you can do to make it stop. If anything makes you feel upset, scared or uncomfortable – tell a trusted adult such as a parent, teacher or someone else you trust.

Never:

- × Never enter incorrect or false information to join social media networks. Age restrictions are in place to protect you from seeing things that may upset you or are there to protect you from risk of harm.

- × Never upload anything that you wouldn't want your parents, teachers or friends to see. Once you send it – it is no longer private.

- × Never create sites, pages or posts that seem to come from someone else. It is wrong to impersonate other people.

- × Never post anything cruel, nasty or offensive even if you are angry about something. You don't know how it will affect someone and you can't take it back. Never spread rumours or post hurtful comments about other people including other pupils and staff at your school. This may be cyberbullying and there could be serious implications for you and the other people involved.

- × Never share personal information like your address or phone number with someone you don't know.

- × Never meet up with people you have met on line – not everyone is who they say they are.

- × Never feel that you are on your own. If there is a problem there are people who can help you. Talk to an adult you can trust.

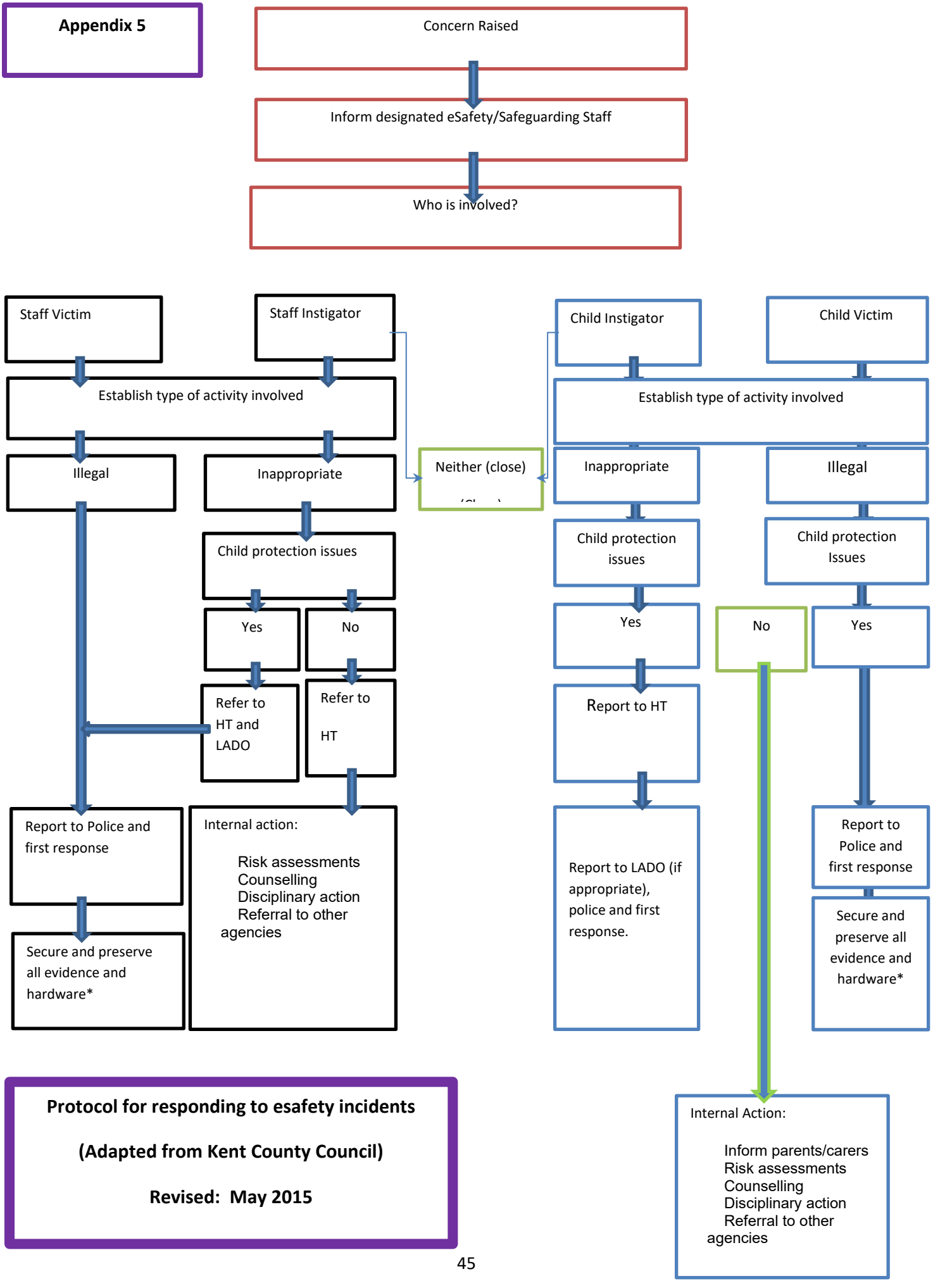
- × Never take or send explicit pictures of yourself, even if you are in a relationship with the person you are sending them to. Once you have sent an image you lost control of who see it and where it goes.

Final Note:

We are proud of our school and all our pupils. Remember we may be monitoring social media and will take seriously any content that could have a negative implication for the school, its staff, its pupils or the community it serves.

I have read the school social media policy and understand my responsibility to comply with requirements set down within it.	
Full name:	
Relationship to School:	Pupil
Signature:	
Date:	

Appendix 5



Protocol for responding to esafety incidents

(Adapted from Kent County Council)

Revised: May 2015

Appendix 6

St Margaret Mary's Catholic Junior School

BUSINESS CONTINUITY ARRANGEMENTS FOR EMERGENCY SITUATIONS

To document alternative ways of working designed to maintain your critical business management and administration activities in the event of a disruption to the ICT Network.

Version Control:

Plan owner:	**Lee Pimblett**
Date:	**June 2022**
Adopted by governing body (date):	**June 2022**
Reviewed (Date):	**June 2023**

This plan should be used to ensure alternative ways of working have been considered, agreed, tested and are fit for purpose.

Circumstances when business continuity strategies may be activated include:

Fire, theft, flood, pandemic, energy loss, loss of internet access, financial implications and Third Party intervention.

This plan is to be used in conjunction with St Margaret Mary's Catholic Junior School Business Continuity/Emergency Plan and the information security policy (or the Data and Information Security: Guidance for Schools V4 where this has been adopted).

A copy of this plan will be kept with the Business Continuity/Emergency plan.

1. Assumptions:

Appropriate forward planning and contingency arrangements ensure that essential business functions can continue in the event of an emergency. The Data Protection Act sets down the legal requirement to secure and protect personal information and effective network management is underpinned by adherence to the recommendations in the Data and Information Security: Guidance for Schools V4.

Consideration should be given to the use of a secure external network, virtualised network or secure cloud that can be accessed via the internet to allow extra back up and protection for files. Contingencies need to be in place to ensure anyone who requires ICT to undertake critical activities has the ability to work at an alternative location.

This plan takes these recommendations into account and the following assumptions apply:

1.1 SIMS (including information held in the individual modules such as staff personnel records and pupil information and contact details) is hosted in the Council's virtual server infrastructure. Information stored in this way benefits from the security, back up and disaster recovery arrangements applied to council applications.

1.2 In the event of an emergency contact information in SIMS is critical in notifying families and in some cases staff. It is essential that this information is reviewed regularly and kept up to date. (Data Protection Act Principles 4 and 5)

1.3 Financial information in SIMS FMS is hosted in the Council's virtual server infrastructure. Information stored in this way benefits from the security, back up and disaster recovery arrangements applied to council applications.

1.4 Electronic information generated on admin machines and stored to either K or S networked drives is backed up to the Council's virtual server infrastructure. Information stored in this way benefits from the security, back up and disaster recovery arrangements applied to council applications. Information saved on device desktops or local hard drive will not benefit from this automated back-up process.

1.5 St Margaret Mary's Catholic Junior School has a current registration with the Information Commissioner's Office which includes the processing of personal information.

1.6 St Margaret Mary's Catholic Junior School has adopted the Information and Data Security: Guidance for Schools V4 or has its own data protection policy which includes requirements for the storage, management and security of electronic information.

1.7 St Margaret Mary's Catholic Junior School has processes in place which ensure staff are aware of and understand their responsibilities in relation to protecting information. Password

policies are in place and access to information is permission restricted according to job role (Data Protection Act Principle 7). (See Information and Data Security Guidance for Schools: Information Security Checklist for Schools). St Margaret Mary's Catholic Junior School has a privacy notice which explains why information is collected and what it is used for (DPA Principle 1).

1.8 Access to the Council's network by schools is governed by the School Network Standards which was adopted on behalf of schools by the Learning Technologies Strategic Board. Managed Service Providers are required to comply with the standards identified in this document.

2. Scenario:

Unable to access the School due to flood, fire, physical threat to the building or danger in the immediate locality, or

Loss of network in school affecting access to business systems and functions.

Description	**Actions to be taken to invoke these arrangements**
Notify parents, carers, governors and other interested parties.	Update school website and social media feeds. These are web-based and accessible from any network. Link to School Business Continuity/Emergency Plan and relocation to alternative premises/buddy school.
Notify LA Senior Manager with responsibility for schools.	Other council services to be notified – links to actions in School Business Continuity/Emergency Plan.
Alert key IT Services who can support access to key systems and information.	Contact IT Managed Service provider. School IT Support will liaise with Corporate IT.
Set up in temporary accommodation.	Link to School Business Continuity/Emergency Plan and relocation to alternative premises/buddy school.
Implement business continuity arrangements at temporary accommodation.	Liaison with IT Managed Service to establish network access at temporary accommodation.

Establish electronic communication.	Access to Outlook email accounts for Head Teacher and administration team (where already set up) are available from any device connected to the council's private network. Office 365 (Web based) accounts provisioned and used in accordance with school policy and security considerations.
Establish connection to management information system.	SIMS applications stored on Council's virtual server infrastructure. Access through Active Directory accounts and therefore available at any location with access to the private network.
Establish connection to financial system.	Financial information held in FMS is stored on Council's virtual server infrastructure. Access through Active Directory accounts and therefore available at any location with access to the private network.
Establish connection to business information generated on school admin devices.	Admin machines on the private network and information stored on shared network drives (K and S Drives) are available through any device on the private network.

Appendix 7

DfE Guidance - Copyright Licencing

This fact sheet provides information for maintained schools, academies and local authorities on copyright licensing in schools for 2015-16.

In 2014-15 the Department managed the copyright licences for all state maintained schools in England that cover print and digital copyright content in books, journals and magazines (Copyright Licensing Agency; CLA); printed music (Schools Printed Music Licence; SPML); licences for copyright content in newspapers and magazines (the Newspaper Licensing Agency media access (NLA) licence); recording and use of copies of radio and television programmes, including from a number of catch-up services (the Educational Recording Agency (ERA) licence) and the showing of films (the Public Video Screening Licence (PVSL) and Motion Picture Licensing Company (MPLC) licences).

Over the past year the Department for Education has been working with the music copyright management organisations (CMOs) to simplify the way in which their copyright licences are paid for by schools and academies. From April 2015 we will add to the above list the licences for the Performing Rights Society for Music (PRS) – payments for performances of covered work; Phonographic Performance Ltd. (PPL) – playing recorded music; the Mechanical Copyright Protection Society (MCPS) – rights to make CDs and DVDs containing copyright music; and Christian Copyright Licensing International (CCLI) – hymns and other Christian music.

Please see below for further information.

Information for Schools

What does this mean for schools?

With the inclusion of these four new licences the Department believes that schools will be covered for almost all their copyright requirements. There are other copyright licences that may be relevant in very specific cases and schools still need to ensure they are covered for any relevant activity. For these ten licences the Department will pay a single sum to each of the CMOs which will cover all primary and secondary schools in England, including academies, and all special schools and Pupil Referral Units. Independent fee paying schools are not licensed in the same way and may wish to seek advice direct from the contacts listed at the end of this briefing. Nursery schools are now included. However, post-16 academies are not included as they are not technically 'schools' and will need to make separate arrangements, as will 6th form colleges.

The licences covered by the new central arrangement are:

1 The CLA licence. This gives you the right to:

- Photocopy books, magazines and journals published in the UK and 30 other countries giving your school access to a wide choice of published information

- Make digital copies by scanning or re-typing for distribution to pupils, parents, teachers or governors, from titles published in the UK and USA plus a growing number of other countries
- Make copies of content from digital material including CD ROMs, electronic workbooks, online journals and included websites
- Use copies with digital whiteboards, VLEs and presentation software programs
- Copy photographs, illustrations, charts or diagrams where they are included in an article or an extract

2 The School Printed Music Licence. This covers the copying and distribution of a school's sheet music to school members for curricular uses and for those extracurricular activities that are not Collective Worship.

The licence permits schools to legally make copies of sheet music by any of the following means:

1. Photocopying
2. Scanning
3. Score-writing software programs
4. Notation by hand
5. Posting on a school VLE

The licence also allows the adaption of the musical work so that it can be performed by any instrumental and vocal arrangements that your school wishes to use.

3 The Newspaper Licensing Agency Schools Licence. This permits the copying of content from national, regional and local newspapers and certain news websites.

4 The Educational Recording Agency licence. This allows educational establishments to record radio and television broadcasts received in the UK and to access copies of such recordings on agreed terms. Teaching staff can also access and download material on a number of on demand catch-up services including BBC iPlayer, 4OD, Five On Demand and ITV Player and Five on Demand. The recordings can then be retained, stored and copied for educational purposes at the licensed establishment. From April 2014 it also allows an educational establishment to enable students to access licensed recordings and clips from them when they are working off site and connect to the schools site.

5 The Public Video Screening Licence. This is issued by Filmbank Distributors Limited who represent all of the six major Hollywood studios in the education sector, (Warner Bros. Sony Pictures, Disney, 20th Century Fox, Universal, Paramount Pictures) and many other leading Hollywood, Bollywood and Independent film studios and distributors including MGM, Lionsgate, Miramax and Entertainment Film. The PVSL is required where schools screen films from studios participating in the PVSL scheme on their premises for entertainment purposes. Under the PVSL scheme schools are able to screen films on DVDs that have been purchased

or borrowed from legitimate UK outlets during the term of the licence. The PVSL does not cover screenings for commercial or fundraising purposes i.e. where a charge is made either directly or indirectly (e.g. selling tickets to screenings). In these circumstances please contact Filmbank directly via info@filmbank.co.uk who can provide you with a licence for this type of screening.

6 The Motion Picture Licensing Company licence. The MPLC licence is similar to the PVSL in that it allows for the non-educational screening of films on the premises of an educational establishment. MPLC represents represent over 400+ film and TV producers and distributors from major Hollywood studios to independent and foreign producers. Examples of the studios whose work is licensed by MPLC are National Geographic; the Discovery Channel; and the studios that own the rights to Bob the Builder and Angelina Ballerina. The MPLC licence does not cover: Commercially advertising the film title outside of the school; making a charge to view the film ; DVDs or downloads that are not a legal copy of the film or Outdoor screenings. If a school does wish to commercially advertise and/or make a charge to view a film, then they should apply for a separate Single Screening MPLC Movie Licence. For further information please visit: http://www.themplc.co.uk/page/film-club-1

7 The Performing Rights Society licence. The PRS licence covers performances of copyright music (including any associated words) which is controlled by The Performing Rights Society Limited (PRS for Music) or by any of the societies in other countries with which PRS for Music is affiliated.

8 The Phonographic Performance licence. The PPL licence is a collective licence authorising a school to play in public, or broadcast, all of its members' recorded music or music videos in the UK. Collective licences can also cover the copying of recorded music and music videos for certain purposes. Typical uses in a school would be: discos/end of term parties; telephone system music on hold; playing a record / radio / tape / CD / digital music player; school fetes (where music is being played) and Dance/Aerobics classes for students and staff only. The two licences are required by every school.

9 The Mechanical Copyright Protection Society licence. The MCPS 'Limited manufacture' licence covers the use of music in DVDs and CDs produced by the school and sold to parents, e.g. by the PTA, to raise funds for the school. The licence provides the right for all schools to make and sell up to 1,000 copies a year of DVDs or CDs containing music.

10 The Christian Copyright Licensing International licence. CCLI administers two licences. The Collective Worship Copyright Licence (CWCL) permits schools to type song words into a computer and store them for later use, e.g. to create a song words database for use with their song projection software; to create service sheets and hand-outs for pupils and staff; to create OHP acetates; and to audio/video record music from services for those unable to attend, or as a keepsake. The Collective Worship Music Reproduction Licence (CWMRL) is supplementary to the CWCL. It permits schools to photocopy the words and music of hymns and worship songs directly from music publications and also to make customised arrangements of music for pupils using transposing instruments (typically wind and brass instruments).

These licences are required either by all (or by the vast majority) of schools and there will be no way for schools to 'opt out' of the licences.

Who is the licensee?

The agreements between the DfE and the CMOs simply covers the administration of the licences. Each education establishment is a Licensee and as such responsible for ensuring that the terms and conditions of the licenses are adhered to by their staff.

Where is my licence?

If you require a copy of your licence, please contact the individual copyright management organisations below.

Information about what the licences cover

What is the SPML and what content is covered?

http://schools.cla.co.uk/your-cla-schools-licence/schools-printed-music-licence/

What is the CLA Licence and what content is covered?

http://schools.cla.co.uk/your-cla-schools-licence/what-can-be-copied/

What is the NLA Licence and what content is covered?

http://schools.cla.co.uk/about-your-licences/nla-schools-licence/nla-licence-documents/

What is the ERA Licence and what content is covered?

General information about the ERA Licence is at: www.era.org.uk

What is the PVSL and what content is covered?

For more information on the PVSL see www.filmbank.co.uk/pvsleducation

For a list of studios participating in the PVSL scheme go to: http://www.filmbank.co.uk/pvslstudios

What is the MPLC licence and what content is covered?

http://www.themplc.co.uk/page/channel-overview-schools

What is the PRS licence and what content is covered?

http://www.prsformusic.com/SiteCollectionDocuments/PPS%20Leaflets/Schools%20leaflet.pdf

What is the PPL licence and what content is covered?

http://www.copyrightandschools.org/

What is the MCPS licence and what content is covered?

http://www.prsformusic.com/Pages/Rights.aspx

What is the CCLI licence and what content is covered?

http://schools.ccli.co.uk/

Does the DfE cover all copyright licences for the sector?

The DfE has agreements with the above CMOs that cover their licences. Other licences may be required by your school for use of other content. More information can be found at: http://www.copyrightandschools.org/

Contacts

Who should I contact?

- Terms and Conditions, rights and repertoire of the CLA, SPML or NLA Licence http://schools.cla.co.uk/get-in-touch/contact-the-schools-team-at-cla/

- Terms and Conditions, rights and repertoire of the ERA licence www.era.org.uk

- Terms and Conditions, rights and repertoire of the PVSL www.filmbank.co.uk/pvslterms.

For information on the PVSL, contact T: 01494 836 231 or email pvsl@cefm.co.uk. The licence terms and conditions for the PVSL can be found at: http://www.filmbank.co.uk/images/80989/pvsl%20terms%20&%20conditions%20feb%202013.pdf.

By screening films from copyright owners licensed under the PVSL scheme, each school, agrees to be bound by and comply with these terms and conditions.

- Terms and Conditions, rights and repertoire of the MPLC http://www.themplc.co.uk/page/contact-the-mplc

- Terms and Conditions of the PPL licence can be found at: http://www.ppluk.com/I-Play-Music/Businesses/Why-do-I-need-a-licence/

- Terms and Conditions of the PRS licence can be found at: http://www.prsformusic.com/users/businessesandliveevents/generaltermsandconditions/Pages/default.aspx

- Terms and Conditions of the MCPS Limited Manufacture licence can be found at: http://www.prsformusic.com/SiteCollectionDocuments/LM%20TandC.pdf

- Terms and Conditions of the CCLI licence can be found at: http://schools.ccli.co.uk/pdfs/schools/terms/SchoolLicenceTermsUK.pdf

- Independent fee paying school licensed through the Independent Association of Prep Schools can obtain advice at https://www.iaps.org.uk/about/copyright-and-schools