St Mary Magdalen's Catholic Primary School

Online Safeguarding Policy

Nurturing Hearts and Minds

Mission Statement

Let the light of Jesus shine through in all we think and say and do.

Contents

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents)
4. Protocol for responding to online safeguarding incidents
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE

1. Introduction and Overview

Definition-What is Online Safeguarding ?

Online Safeguarding, Online Safety, Digital Safety, online safeguarding and Internet Safety are all terms used to varying extents to describe staying safe online. In recent years, the breadth and variety of issues has increased significantly and by its nature, is an agenda that will continue to evolve, none more so than the impact of Social Media. Specific risk areas within Online Safeguarding are varied and evolving and includes (but is not limited to) Online Child Sexual Exploitation, Bullying, Gaming, Sexting and Online Radicalisation amongst others.

Addressing potential issues around the online environment presents a variety of challenges for us. Whether we are Parents/Carers, Schools/Colleges, Youth Groups, Police, Local Authorities, Health professionals or any number of other individuals or organisation with an interest in keeping our Children and Young People safe online, it is key that we recognise that whatever particular risk area we are addressing, it remains a Safeguarding issue at its core. This is reflected in the definition of Online Safeguarding as:

"a Safeguarding issue where technology is involved"

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Mary Magdalen's Catholic Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St Mary Magdalen's Catholic Primary School.
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- have clear procedures for handling personal data
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:
Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)

copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope
This policy applies to all members of St Mary Magdalen's Catholic Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St Mary Magdalen's.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safeguarding incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safeguarding behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for online safeguarding • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL • To be responsible for ensuring that staff and volunteers receive suitable training to carry out their online safeguarding roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online child protection incident. • To ensure that there is a system in place to monitor and support staff who carry out internal online safeguarding procedures (e.g. network manager) • Ensure that all staff and volunteers read this policy and sign the acceptable use agreement before starting work or placement • To ensure that all data held on pupils on the school office machines have appropriate access controls in place • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.

Online safeguarding Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the school online safeguarding policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that online safeguarding education is embedded across the curriculum
	• Liaises with school IT technical staff
	• To communicate regularly with SLT and the designated IT Governor to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safeguarding incident
	• To ensure that an online safeguarding incident log is kept up to date
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in online safeguarding issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Role	Key Responsibilities
Governors/ ICT Governor	• To ensure that the school follows all current online safeguarding advice to keep the children and staff safe. • To approve the online safeguarding Policy and review the effectiveness of the policy. This will be carried out by the Pupils and Curriculum Committee. • To write a brief safety report in the summer term. • To support the school in encouraging parents and the wider community to become engaged in online safeguarding activities.
Computing Curriculum Leader	• To oversee the delivery of the online safeguarding element of the Computing curriculum. • To liaise with the online safeguarding coordinator regularly .
Network Manager/technician	• To report any online safeguarding related issues that arises, to the Headteacher. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are used responsibly. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date). • To ensure the security of the school ICT system. • To ensure that web filtering is applied and updated on a regular basis. • To inform Virtue of issues relating to the filtering applied by the Grid. • To keep up to date with the school's online safeguarding policy and technical information in order to effectively carry out their online safeguarding role and to inform and update others as relevant. • To monitor the use of the network remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures.
Teachers	• To embed online safeguarding issues in all aspects of the curriculum and other school activities . • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's online safeguarding policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy. • To be aware of online safeguarding issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • To read, understand, sign and adhere to the Mobile Phone Policy. • To read, understand, sign and adhere to the school's Staff Handbook. • To report any suspected misuse or problem to the online safeguarding coordinator. • To maintain an awareness of current online safeguarding issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safeguarding practice when using digital technologies out of school and realise that the school's Online safeguarding Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home. • To help the school in the creation/ review of online safeguarding policies and charters.

Role	Key Responsibilities
Parents/carers	• To support the school in promoting online safeguarding and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children. • To access the school website and school on line learning sites (i.e. Sum Dog) with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school.

Communication:
How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and staff area of the website.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

Handling complaints:

- The school will take all reasonable precautions to ensure online safeguarding. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material 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 of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - interview/counselling by teacher the online safeguarding Coordinator / Headteacher.
    - informing parents or carers.

- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework].
- referral to LA / Police.

- Our online safeguarding Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The online safeguarding policy is referenced from within other school policies: Child Protection policy and Anti-Bullying policy.

- The school has an online safeguarding coordinator (Mrs Gallagher) who will be responsible for document ownership, review and updates.
- The online safeguarding policy will be reviewed every three years or when any significant changes occur with regard to the technologies in use within the school.
- The online safeguarding policy has been written by the school online safeguarding Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

Version Control

As part of the maintenance involved with ensuring your online safeguarding policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	St Mary Magdalen's Catholic Primary School online safeguarding policy

Version	2.0
Date	06/03/2018
Author	online safeguarding coordinator
Approved by head teacher	D Gallagher
Approved by Governing Body	Summer 2018
Next Review Date	Summer 2021

Modification History			
Version	Date	Description	Revision Author
0.1	12/09/2013	Initial draft	online safeguarding coordinator
2.0	06/03/2018	Version responding to KSIE Sept 2016	Diane Gallagher

2. Education and Curriculum

Pupil online safeguarding curriculum

This school

- Has a clear, progressive online safeguarding education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL e-Safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy.
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may 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 acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour. keeping personal information private.
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and 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.
    - [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. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups. buying on-line. on-line gaming / gambling.

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on online safeguarding issues and the school's online safeguarding education program. staff meetings, staff briefings, staff area of website.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.
    - Information leaflets. in school newsletters. on the school website. prospectus
    - demonstrations, practical sessions held at school.
    - suggestions for safe Internet use at home.
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should understand the importance of adopting good online safeguarding practice when using digital technologies out of school and realise that the school's Online safeguarding Policy covers their actions out of school, if related to their membership of the school.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- are responsible for reading the school's online safeguarding policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safeguarding acceptable use agreement form at time of their child's entry to the school.
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safeguarding policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safeguarding issues.
- monitoring and reporting of online safeguarding incidents takes place and contribute to developments in policy and practice in online safeguarding within the school. The

records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB.

- parents / carers are specifically informed of online safeguarding incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through Virtue technologies and so connects to the 'private' National Education Network.
- Uses the Sophos complete security filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.
- Ensures network health through use of Sophos anti-virus software and network set-up so staff and pupils cannot download executable files.
- Uses DfE or LA approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- 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 / Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable / useful.
- Works in partnership with Virtue to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form 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 not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required. eg yahoo for kids or ask for kids , Google Safe Search , …..

- Never allows / 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 students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider at All Hallows or Virtue Helpdesk as necessary.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  This school
  - Uses individual, audited log-ins for all users.
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
  - Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful.
  - Has additional local network auditing software installed.
  - Ensures the Systems Administrator / network manager is up-to-date with Virtue services and policies / requires the Technical Support Provider to be up-to-date with Virtue services and policies.
  - Storage of all data within the school will conform to the UK data protection requirements.

    Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the staff code of conduct for ICT. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- We provide pupils with an individual folder assigned to their class on the Linkstation.
- Makes clear that no one should access another person's folder without permission.

- Has set-up the network with a shared work 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 always log off when they have finished working or are leaving the computer unattended.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- We discourage pen drives being used in school.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies.
  e.g. Borough email or Intranet. finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed to the best of their ability.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role.
  e.g. teachers access report writing module. SEN coordinator - SEN data.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password).
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements.

- Uses the DfE 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 LA or through USO secure file exchange (USO FX).
- 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 suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, LGfL admin site, regularly.

E-mail

This school

- Provides staff with an email account for their professional use, *lancs.sch.uk email* and makes clear personal email should be through a separate account. Once an email has been issued we will not correspond with private emails.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of Virtue-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for

viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, Virue filters, monitors and protects our internet access to the World Wide Web.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils are taught about online safeguarding and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
    - that an e-mail is a form of publishing where the message should be clear, short and concise.
    - that any e-mail sent to an external organisation should be written carefully 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 e-mail, such as address, telephone number, etc.
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.
    - that they should think carefully before sending any attachments.
    - embedding adverts is not allowed.
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
    - not to respond to malicious or threatening messages.
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
    - that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff are encouraged to only use the school e mail systems- office 365.
- Staff are encouraged to only use 365 e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. We use secure approved systems. These include: S2S (for school to school transfer). Collect. USO-FX, CPOMs
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- the sending of chain letters is not permitted.
- embedding adverts is not allowed.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to office and teaching staff.
- The school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work. where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published.
- Photographs published on the web 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 expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

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 risk of loss of personal information.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).

- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All classroom based and office staff should log meetings, incidents, welfare concerns
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - staff,
    - governors,
    - pupils
    - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after a short time
- We use encrypted hard drives if any member of staff has to take any sensitive information off site. However this will be rare as files can be accessed remotely.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use CPOMs to transfer child protection documents if the receiving school also uses CPOMs.
- Staff have portal accounts with different levels of access.
- We use VPN solution with its 2-factor authentication for remote access into our systems.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.

- We use Virtues' remote secure back-up for disaster recovery on our admin and curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the school office on arrival at school. Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided. except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. If a staff member is expecting an important personal call they may seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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 then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use

their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their online safeguarding education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with 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 data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in an electronic inventory.
.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Acceptable Use agreements

The agreements in the appendices will be issued to parents electronically.

Appendix 1- Letter to parent re image consent

Image Consent Form

Dear Parent / Carer

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website/VLE, or in school displays, including digital photo frames. (*List any other specific uses here)*.

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

Yours sincerely,

Mrs D Gallagher

Headteacher

Appendix 2-Image consent form

Image Consent Form

Name of the child's parent/carer:……
Name of child:……
Year group:……

Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (one for each child) should be returned to school as soon as possible.
(Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school?
   Yes / No

2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra curricular events? Yes / No

3. May we use your child's image in printed school publications and for digital display purposes within school?
   Yes / No

4. May we use your child's image on our school's online publications e.g. website / blog / VLE?
   Yes / No

5. May we record your child on video? Yes / No

6. May we allow your child to appear in the media as part of school's involvement in an event?
   Yes / No

I have read and understand the conditions of use attached to this form

Parent/Carer's signature:

……

Name (PRINT):

……

Date: ……..

Conditions of Use

1. This form is valid for the time your child is at St Mary Magdalen's However consent can be withdrawn at any time. This must be done in writing..
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.
8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).
3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

Appendix 3- Letter and consent form re third party images

Consent Form for Images to be Taken e.g. at a School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in our school productions throughout their time at school. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images / video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage. Should any parents / carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.

These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely

Mrs Gallagher

Child's name: _____ Date: _____

I agree / do not agree to photographs / videos being taken by third parties in school events and productions.

Signed _____ *(Parent / Carer)*

Print name _____

Appendix 4 –AUP- Staff

St Mary Magdalen's Catholic Primary School

ICT Acceptable Use Policy
Staff and Governors

Jesus let your light shine through, in all we think and say and do

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of <*insert name*>.

10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name ……(PRINT)

Position/Role ……

Appendix 5 –AUP -Visitors

St Mary Magdalen's Catholic Primary School

ICT Acceptable Use Policy – Students, Supply Teachers, Visitors, Guests etc.

Jesus let your light shine through, in all we think and say and do

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……

Date ……

Full Name ……(PRINT)

Position/Role ……

Appendix 6 –AUP Children

St Mary Magdalen's Catholic Primary School

ICT Acceptable Use Policy (AUP) - Children

Jesus let your light shine through, in all we think and say and do

These rules reflect the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class e-mail address or my own school email address when emailing.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will not deliberately bring in inappropriate electronic materials from home.
- ✓ I will not deliberately look for, or access inappropriate websites.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own, or others', details such as names, phone numbers or home addresses.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will not arrange to meet anyone that I have met online.
- ✓ I will only open/delete my own files.

- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.
- ✓

……

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and

…… [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at St Mary Magdalen's

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class ……

Date……

This AUP must be signed and returned at the beginning of the juniors.

Appendix 7 – Letter to parent regarding AUP

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing eSafety as part of your child's learning, we will also be holding Parental eSafety Awareness Sessions periodically and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about eSafety for parents and carers, please visit the school website parent information section. http://www.st-marymagdalen.lancs.sch.uk/parents/e-safety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact me.

Yours sincerely,

Mrs D Gallagher

Headteacher