ST MARGARET CLITHEROW PRIMARY SCHOOL

We live to love, learn, respect
and follow Jesus who says,
“Love one another as I have loved you.”

Online Safety Policy

Legal Status: Statutory
Version Date: February 2013
Last Review: November 2016
Next Review: November 2017
Responsible Person: Governing Body

Table of Contents

1. Introduction and Overview

Rationale behind the policy

The purpose of this policy is to:

- set out the key principles expected of all members of St. Margaret Clitherow's Primary community with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of St. Margaret Clitherow's Primary.
- 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 cyber bullying which are cross referenced with other school policies.
- 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 pupils.

The main areas of risk for our school community

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.)

(Ofsted Inspecting Online Safety guidance for inspectors, 2013)

Scope of this policy

This policy applies to all members of St.Margaret Clitherow's community (including staff, pupils, governors, volunteers, parents, carers, visitors and community users) who have access to and are users of the school IT systems both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, 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. 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 Bullying Prevention Policy and will, where known, inform parents and carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Role	**Key Responsibilities**
Head teacher	• Takes overall responsibility for Online Safety provision • Takes overall responsibility for data and data security (SIRO) • Ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements (in St.Margaret Clitherow's case the London Grid for Learning) • Is responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant • Aware of procedures to be followed in the event of a serious Online Safety incident. • Receives timely monitoring reports from the Online Safety Lead.
Online Safety Lead / Designated Child Protection Lead	• Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies and documents • Promotes an awareness and commitment to safeguarding throughout the school community • Ensures that Online Safety education is embedded across the curriculum • Liaises with school IT technical staff • Communicates regularly with SLT and the designated Online Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • Ensures all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • Ensure that an Online Safety 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 Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data

Role	Key Responsibilities
	• access to illegal or inappropriate materials • inappropriate on-line contact with adults and strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Governors / Online Safety governor	• Ensures that the school follows all current Online Safety advice to keep children and staff safe • Approves this Online Safety Policy and reviews the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor • Supports the school and wider community to engage in Online Safety activities
Computing Leader	• Oversees the delivery of the Online Safety element of the Computing curriculum • Liaises with the Online Safety Lead regularly
Technician	• Reports any Online Safety related issues that arise, to the Online Safety Lead. • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • Ensures the security of the school ICT system • Ensure that access controls and encryption exist to protect personal and sensitive information held on school-owned devices • Manages the day-to-day web filtering of the school • Informs the LGfL of any issues relating to the filtering • Keeps up to date with this policy and technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant • Supports the monitoring of network use, remote access, online storage and email and reports any misuse to the Online Safety Lead for further investigation • Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • Keeps up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
LGfL Nominated Contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
Teachers	• Embed Online Safety in all aspects of the curriculum and other school activities • Supervise and guide pupils carefully when engaged in learning activities involving online technology, including extra-curricular and extended school activities • 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 Safety policy and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of Online Safety 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 report any suspected misuse or problem to the Online Safety Lead • To maintain an awareness of current Online Safety 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 Pupils' Acceptable Use Agreement (At KS1 parents are expected to sign on behalf of pupils) • Demonstrate a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology • Know and understand school policy on the use of mobile phones, digital cameras and hand held devices • Recognise that the misuse of images could be a form of cyber-bullying • Understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety 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 and review of Online Safety policies
Parents and carers	• Support the school in promoting Online Safety 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 • Read, understand and promote the school Pupil Acceptable Use Agreement with their children • Access the school's website, blogging platform and any pupil records in accordance with the relevant school Acceptable Use Agreement • To consult with the school if they have any concerns about their children's use of technology

How the policy will be communicated to staff, pupils and the community

- This policy will be posted on the school website and a copy will be made available in the staffroom
- Acceptable Use Agreements will be signed (where age-appropriate) and 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 or by the Subject Leader.

Review and Monitoring

The Online Safety policy is referenced from within other school policies: Computing policy, Child Protection Policy, Bullying Prevention policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an Online Safety Lead who will be responsible for document ownership, review and updates.
- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The Online Safety Policy has been written by the school Online Safety Lead 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.

2. Education and Curriculum

Pupil Online Safety curriculum

St.Margaret Clitherow's Primary School

- Has a clear, progressive Online Safety education programme as part of the Computing curriculum. It is based on the London Grid for Learning Digital Literacy and Online Safety Scheme and the school's preferred curriculum support provider (currently 3BM Education Partners.) 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;
  - to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - use of child-friendly search engines where more open Internet searching is required; e.g. KidRex, PrimarySchoolICT or Google's Kids SafeSearch;
  - to understand acceptable behaviour when using an online environment or email, i.e. be polite, no rude 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;
- 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.
- reminds pupils about their responsibilities through an Acceptable Use Agreement which every pupil signs and through Internet rules displayed throughout the school.
- encourages staff to model safe behaviours 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

St.Margaret Clitherow's Primary 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 annual training available to staff on Online Safety issues and the school's Online Safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on Online Safety and expects them to sign an Acceptable Use Agreement.

Parent awareness and training

St.Margaret Clitherow's Primary School

- runs a rolling programme of advice, guidance and training for parents, including:
- signing of the "Parents' and Pupils' Acceptable Use Agreements" as part of the induction process for new parents – the principles of e-safe behaviour are made clear;

- information leaflets, in particular the latest copies of the Vodafone Digital Parenting magazine;
- updates in school newsletters;
- guidance on parent support materials on the school web site;
- demonstrations, practical sessions held at school;
- suggestions for safe internet use at home via the school website and newsletters;
- provision of information about national support sites for parents via the school website.

3. Expected Conduct and Incident management conduct we expect

All users

are responsible for using the school IT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign;
understand the consequences of misuse or access to inappropriate materials;
understand the importance of reporting abuse, misuse or access to inappropriate materials and are aware of how to do so;
understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that this Policy covers their actions out of school, if related to their membership of the school.

Staff

are responsible for reading this policy, signing the Acceptable Use Agreement and using the school IT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

should have a good understanding of Online Safety, including research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

give consent for pupils to use the internet, as well as other technologies, as part of the Acceptable Use Agreement;

Incident Management

At St.Margaret Clitherow's Primary School

There is strict monitoring and application of the this policy and an 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 (e.g. the local authority, London Grid for Learning and/or the UK Safer Internet Centre helpline) in dealing with Online Safety issues;
Monitoring and reporting of Online Safety incidents takes place and contribute to developments in policy and practice in Online Safety within the school. The records are reviewed and reported to the school's senior leaders and governors; parents / carers are specifically informed of Online Safety 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;
we use the various sanctions that are detailed in the school's Behaviour Policy; these assign incidents a colour code of green, amber or red with appropriate sanctions attached to each.

Handling complaints

- The school will take all reasonable precautions to ensure Online Safety. 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 Online Safety Lead and/or the Headteacher;
  - informing parents or carers;
  - any sanctions as detailed in the current Behaviour Policy;
  - any sanctions as detailed in the current Bullying Prevention Policy;
  - removal of Internet or computer access for a period;
  - referral to the Local Authority Designated Officer (LADO) or the police.
  - Our Online Safety Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred directly to the Headteacher.
  - Complaints of cyberbullying are dealt with in accordance with our Bullying Prevention Policy.
  - Complaints related to child protection are dealt with in accordance with our Child Protection Policy.

4. Managing the IT infrastructure

St. Margaret Clitherow's Primary School website

- the Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- the school web site complies with the statutory DfE guidance, as amended in 2014 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 our main contact email address of **admin@clitherow.brent.sch.uk;**
- photographs published on the web do not have full names of pupils attached;
- we do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Internet access, virus protection and filtering

St. Margaret Clitherow's Primary School

- has the educational filtered secure broadband connectivity through the London Grid for Learning and so connects to the 'private' National Education Network;
- uses the LGfL Net Sweeper 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;
- ensures network integrity through the use of Sophos anti-virus software (from LGfL;)
- blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- 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;
- is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- ensures pupils only publish their learning within an appropriately secure environment such as the school's blogging site www.stpeterscelbhf.j2webby.co.uk;
- requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's easy.uso.im online tool as a key way to direct pupils to age and subject appropriate web sites;
- informs staff and pupils that that they must report any failure of the filtering systems directly to the e-
- Safety Lead who will log or escalate as appropriate to the Technical service provider;
- makes clear all users know and understand what the Acceptable Use Agreement rules of use are and what sanctions result from misuse – through staff meetings and teaching programme;
- immediately refers any material we suspect is illegal to the appropriate authorities – Police/LADO.

Video Conferencing

- we only use the LGfL supported services for video conferencing activity;
- we only use approved or checked webcam sites;

Closed Circuit Television (CCTV)

- we have CCTV in the school as part of our site surveillance for staff and pupil safety. We will not reveal any recordings (retained by the Support Provider for 28 days,) without permission except where disclosed to the Police as part of a criminal investigation.

Social Networking

- See separate Social Media Protocol.

Network management (user access and backup)

To ensure St. Margaret Clitherow's network is used safely, we

- use guest accounts for short term visitors for temporary access to appropriate services;
- use teacher 'remote' management control tools for controlling workstations / viewing users;

- ensure the Technical Support Provider is up-to-date with LGfL services and policies;
- store all data within the school securely, conforming to the UK data protection requirements;
- ensure staff read and sign an Acceptable Use Agreement. Following this, they are set-up with Internet, email access and network access. Online access to services is through a unique, audited username and password. We also use the same username and password for access to our school's network;
- provide Key Stage 2 pupils with an individual network log-in username;
- issue all pupils have their own unique username and password which gives them access to a range of online resources that we or the LGfL have approved;
- ensure that pupils in Key Stage 1 and KS2 sign an Acceptable Use Agreement;
- make clear that no one should log on as another user and that pupils should never be allowed to log-on or staff logins as these could be mis-used;
- have set-up the network with a shared work area for pupils and one for staff;
- have set-up the network so that users cannot download executable files / programmes;
- have blocked access to music, media download or shopping sites – except those approved for educational purposes;
- have up-to-date anti-virus software on all our devices;
- make 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 – there is a separate Loan Agreement for staff;
- make 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;
- maintain equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers;
- ensure that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems;
- do not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and only through approved systems, such as CentraStage;
- provide pupils and staff with access to content and resources through the LGfL my.uso.im & easy.uso.im platform which staff and pupils access using their USO username and password;
- make clear responsibilities for the daily back up of MIS and finance systems and other important files;
- have 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;
- our wireless network has been secured to appropriate standards suitable for educational use;
- reviews the school IT systems regularly with regard to health and safety and security.

E-mail

St. Margaret Clitherow's Primary School staff

- use LGfL StaffMail email accounts for their professional role; personal emails are through a separate account;
- does not publish personal e-mail addresses of staff on the school website;
- know that spam, phishing and virus attachments can make e-mails dangerous. We use a number of LGfL-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, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.
- never use email to transfer staff or pupil personal data. We use secure, approved systems which include S2S (for school to school transfer) and the LGfL USO-FX service;

- know that e-mail sent to an external organisation must be written carefully and considerately and may require authorisation from the SLT.

St. Margaret Clitherow's Primary pupils

- use a simulated emailing environment while in KS1 (using 2Simple's 2Email) and while in KS2 an LGfL LondonMail account with SafeMail rules controlling content;
- e-mail accounts are intentionally 'anonymised' for their protection.
- are introduced to, and use e-mail as part of planned Computing curriculum.
- can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- sign, where age-appropriate, the Acceptable Use Agreement to say they have read and understood the Online Safety rules regarding use of e-mail.
- are taught about the '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;
  - that they must immediately tell a teacher / trusted adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond or delete malicious or 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 trusted adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.

5. Data security

Strategic and operational practices

At St. Margaret Clitherow's Primary

- the Head Teacher is the Senior Information Risk Officer (SIRO);
- we ensure staff know who to report any incidents where data protection may have been compromised;
- all staff are DBS checked and records are held in one central record within SIMS.
- we ensure all staff, governors, parents and pupils sign an Acceptable Use Agreement form and monitor who has signed. The AUP makes clear staffs' responsibilities with regard to data security, passwords and access.

Technical Solutions

St. Margaret Clitherow's Primary

- staff have access to a Staff Shared drive where sensitive documents and photographs can be stored;
- discourage the use of flash drives and USB sticks, instead advising to use LGfL's My Drive;
- use the DfE S2S site to securely transfer CTF pupil data files to other schools;

- use the Pan-London e-Admissions system (based on USO FX) to transfer admissions data;
- use the LGfL approved remote access solution so staff can access sensitive and other data from home, without the need to take data home;
- use the LGfL's Unified Sign On File eXchange (USO FX) to transfer other data to schools in London, such as references, reports of children;
- uses the DfE, LA or LGfL approved systems such as USO FX 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;
- all servers are in lockable rooms managed by DBS-checked staff;
- we use the LGfL Gridstore product for disaster recovery, which securely backs up our admin and curriculum servers each night using our internet connection. The data is hosted in several secure data centres within the UK to comply with data protection laws;
- 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 and obtain a certificate of secure deletion for any server that once contained personal data;
- paper based sensitive information is shredded, using a cross cut shredder.

Password policy

St.Margaret Clitherow's Primary 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;
- staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- require staff to use strong and unique usernames for access into our MIS system – these are different .

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils' & parents' or visitors own risk – St. Margaret Clitherow's Primary School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought onto school premises.
- All visitors to our school are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on school property without the knowledge of the person(s) being recorded is strictly prohibited.
- 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. Any such incidents may require police attendance.
- Where parents or pupils need to contact each other during the school day, they should do so only through the School's main phone number. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or 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.
- 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.

Pupils' use of personal devices

- Only children in Years 5 & 6 are allowed to bring their own mobile phones to school. These are then handed to Mrs Haneef or Mrs Khan on Reception for the duration of the day and are collected at the end of the school day.
- 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. Please contact the headteacher if you wish to discuss this.
- If a pupil 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.
- If a pupil 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.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils 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 pupils, 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 the teaching day unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils under any circumstances.
- 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 pupils 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 their own mobile number for confidentiality purposes by preceding any number called with 141.

Digital images and video

At St. Margaret Clitherow's School

- we gain parental / carer permission for use of digital photographs or video involving their child as part of the Acceptable Use Agreement form as part of new parent induction;
- we do not identify pupils in online photographic materials (if a name is used, then no photograph or if a photograph is used, no name;_
- staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- pupils are taught about how images can be manipulated in their Online Safety education curriculum 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 Computing lessons;
- 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.

Other related documents and policies to be read in conjunction with this policy

1. Staff, Governors and Volunteers Acceptable Use Agreement 2016-17.
2. Pupils' Acceptable Use Agreement 2016-17.
3. Behaviour Policy.
4. Anti-Bullying Policy.