St Agatha's Catholic Primary School

Policy	**Online Safety Policy**
Author	**Elizabeth Cahill**
Date	**September 2025**
Date of Review	**September 2026**
Governor Committee	**CFCF**
Statutory Policy	**Y/N**

1. Introduction and Overview

1.1 The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St. Agatha's Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of St. Agatha's Primary School in relation to safe use of the internet.
- 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 online 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 children.

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

2.1 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

2.2 Contact

- Grooming
- Online-bullying in all forms
- Identity theft (including 'frape' (hacking Social media profiles)) and sharing passwords

2.3 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)

This policy applies to all members of St. Agatha's Primary School community who have access to and are users of school ICT systems, both in and out of St. Agatha's Primary School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children 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 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 electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's published Pastoral Care 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 behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for online provision • To take overall responsibility for data and data security (SIRO) • To take a lead on filtering and monitoring arrangements including ensuring that the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL and that all staff receive appropriate training • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online Safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator and report/meet with the Online Safety Link Governor and FGB • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)

Role	Key Responsibilities

Online Safety Co-ordinator	Under guidance of the DSL (Headteacher) and deputy DSL (Deputy Headteacher):
	• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
	• promotes an awareness and commitment to online safeguarding throughout the school community
	• ensures that online safety education is embedded across the curriculum
	• liaises with school ICT manager
	• to communicate regularly with SLT 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 Safety incident
	• to ensure that an Online Safety incident log is kept up to date on CPOMS
	• 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
	  • 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

Governors / Online Safety Governor	• To ensure that the school follows all current Online Safety advice to keep the children and staff safe • To approve the Online Safety Policy and review 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 • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinator / Officer (including online safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety/Child protection leader regularly • that he / she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
Network Manager/technician (ClickIT)	• To report any online safety related issues that arises, to the child protection leader.

Role	Key Responsibilities
	• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • 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 access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • that the use of the *network / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *On-line Safety Co-ordinator / Officer /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 online security and technical procedures • To ensure that all data held on children in the school office machines have appropriate access controls in place
Teachers	• To be trained in cyber security – annual with regular updates • To fulfil their role in relation to filtering and monitoring in line with training and updates • To embed online safety issues in all aspects of the curriculum and other school activities, especially through the 'Switched on' Computing scheme and emphasis of this during Online Safety week. • 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.
All staff	• To read, understand and help promote the school's Online Safety policies and guidance written in line with the school's Safeguarding Policy. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • 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 coordinator • 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

Role	Key Responsibilities
	• 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.
Children	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • Do not share personal information online • Only bring mobile phones and smart technology onto school premises in line with the mobile phone policy • 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 online-bullying. • To 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/ review of safety policies
Parents/carers	• To 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 and parents' use of photographic and video images • To read, understand and promote the school's Child Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology • To air concerns / complaints off line and directly with school following published procedures
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

3. Education and Curriculum

3.1 Children's Online Safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum. 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 children] 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 that anything they post is traceable back to them;
    - 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 children] 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 children about their responsibilities through an end-user Acceptable Use Policy which every child 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 children 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 children 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;

3.2 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 safety issues and the school's e-safety education program
- Provides, as part of the induction process, all new staff and governors [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.
- Ensures that governors have sufficient knowledge to be able to challenge appropriately.

3.3 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 online safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

4 Expected Conduct and Incident management

4.1 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 children.
- 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 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

- 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 safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand-held devices.

Children

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

Parents/Carers

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

4.2 Incident Management

In this school:

- there is strict monitoring and application of the online safety 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 (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety 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 safety incidents involving children for whom they are responsible.
- We will contact the police if one of our staff or children receives online communication that we consider is particularly disturbing or breaks the law

5. Managing the ICT infrastructure

5.1 Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL 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 are 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 children;
- Ensures network health through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL 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 the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of children's use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older children have more flexible access;
- Ensures all staff and children have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures children only publish within an appropriately secure environment: the school's learning environment/ the London LEARNING PLATFORM/ LGfL secure platforms such as J2Bloggy, etc
- 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 children 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; e.g. ask for kids and Google Safe Search
- Is vigilant when conducting 'raw' image search with children e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and children that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL 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 children, 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 - the London USO system;
  - 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 LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
  - Storage of all data within the school will conform to the UK data protection requirements

    Children 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 and governors have read and signed that they have understood the school's online safety Policy. 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. We also *provide a different / use the same username and password* for access to our school's network;

- Staff access to the school's management information system is controlled through a separate password for data security purposes;

- Provides children with an individual network log-in username. From Year 3 they are also expected to use a personal password;

- In KS2, children have their own unique username and password which gives them access to the Internet, the Learning Platform *and (for older pupils) their own school approved email account*;

- Uses the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;

- Makes clear that no one should log on as another user and makes clear that children should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

- Has set-up the network with a shared work area for children 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;

- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 15 mins and have to re-enter their username and password to re-enter the network.];

- 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;

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

- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;

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

- Makes clear that staff are responsible for ensuring that 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;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers

- 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 children and staff with access to content and resources through the approved Learning Platform, which staff and children access using their username and password (their USO username and password);

- Assigns 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 child 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

- This school makes it clear that staff and children 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. Staff change their passwords on a regular basis.

E-mail

This school:

- Provides staff and governors with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account;
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses Londonmail with students as this has email content control
- Does not publish personal e-mail addresses of children, governors or staff on the school website. We use anonymous or group e-mail addresses, for example info@stagathas.school 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 children 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

Children:

- We use LGfL LondonMail with children and lock this down where appropriate using LGfL SafeMail rules.
- Children's LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Children are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Year R/1 children are introduced to principles of e-mail through the Visual Mail facility in the London LEARNING PLATFORM OR closed 'simulation' software.
- Children can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Children are taught about the safety 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 have only met online without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

- Children sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Can only use the LA or LGfL e mail systems on the school system
- Only use LA or LGfL 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 children's personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX*, named LA system;*
- 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;

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.

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

School staff will ensure that in private use:

- No reference should be made in social media to children, parents, carers, governors 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 /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Children's use of personal devices

- The School strongly advises that children's mobile phones and smart technology should not be brought into school. Special arrangements for older children may be arranged on an individual basis.
- If a child breaches the school's policy then the phone or smart device may be confiscated and held in a secure place in the school office. Mobile phones and smart devices will be released to parents or carers in accordance with the school policy.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or smart devices for taking photos or 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 e.g. trips.
- Mobile Phones and personally-owned smart 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 or in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones, smart technology devices or cameras, to take photos or videos of children and will only use work-provided equipment for this purpose.
- 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 children 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 children;
- If specific children's 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/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Children 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 identify 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.