E- Safety Policy

Date Governors Agreed:	18th January 2018
Date to be next reviewed:	January 2019
Head Teacher signature:	
Chair of Governors signature:	

South Grove Primary School E-Safety Policy 2018-2019

Contents

1. **Introduction and overview**
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy be communicated to staff/pupils/community
   - Handling complaints
   - Review and Monitoring

2. **Education and Curriculum**
   - Pupil e-safety Curriculum
   - Staff and governor training
   - Parent awareness and training

3. **Expected Conduct and Incident management**

4. **Managing the ICT infrastructure**
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Passwords policy
   - E-mail
   - School website
   - Learning platform
   - Social networking
   - Video Conferencing

5. **Data security**
   - Management Information System access
   - Data transfer

6. **Equipment and Digital Content**
   - 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 e-safety incidents http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

1. Introduction and Overview

Rationale
The purpose of this policy is to:
- Set out the key principles expected of all members of the school community at South Grove Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of South Grove 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 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.
- 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))

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

Scope
This policy applies to all members of South Grove Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of South Grove Primary School.

Role	Key Responsibilities
Head Teacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

E-Safety Co-ordinator and Designated Child Protection Leader	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT to discuss current issues, review incident logs and filter control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• Facilitate training and advice for all staff
	• Oversee any pupil surveys / pupil feedback on online safety issues
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and is 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 strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: Regular review with the E-Safety Co-ordinator
Computing Co-ordinator	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the Child protection leader regularly

South Grove E-Safety Policy January 2018-2019
LGFL Version 2016

Role	Key Responsibilities
ICT technician	• To report any e-safety related issues that arises, to the E-Safety coordinator. • 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 ICT technician keeps up to date with the school's E-Safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • That the use of the local network, Virtual Learning Environment, and other internet resources is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator for investigation. • 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
Data Manager	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
LGfL Nominated contact	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed e-safety 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
All staff	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement and E-safety policy, and understand any updates annually. The AUP is signed by new staff on induction. • To be aware of e-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 E-Safety coordinator • To maintain an awareness of current e-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. **Exit strategy** At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with technician on the last day to

Role	Key Responsibilities
	log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use 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 understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of 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 contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To support the school in promoting e-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 • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website 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
External groups Including parent groups	• Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed and signed 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
- Regular updates and training on online safety for all staff.

Handling incidents:
- The school will take all reasonable precautions to ensure e-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:

- o   interview/counselling with the E-Safety Coordinator or Headteacher;
- o   informing parents or carers;
- o   removal of Internet or computer access for a period of time
- o   referral to Local Authority/Police
- Our E-Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day

- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

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

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- 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 safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil E-safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing and PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online 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 the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and Governor training
This school

- makes regular training available to staff on e-safety issues and the school's e-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 the e-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:
  - o Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - o Information leaflets; in school newsletters; on the school website;
  - o demonstrations, practical sessions held at school;
  - o suggestions for safe Internet use at home;
  - o provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct
In this school, all users:
- o 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.
- o understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- o understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so
- o understand the importance of adopting good e-safety practice when using digital technologies out of school
- o know and understand school policies on the use of mobile phones, digital cameras and hand held devices.

Staff, volunteers and contractors
- know to be vigilant in the supervision of children at all times
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers
- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management
In this school:
- o there is strict monitoring and application of the E-Safety policy and a differentiated and appropriate range of sanctions
- o 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.
- o support is actively sought from other agencies as needed e.g. the local authority (London Borough of Waltham Forest) and regional broadband grid (London Grid for Learning), UK Safer Internet Centre helpline in dealing with e-safety issues
- o monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders.
- o parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- o 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
- o We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and and Communication System

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

This school:
- o Has the educational filtered secure broadband connectivity through the LGfL

- o Uses a proprietary dedicated Proxy Filtering Server which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.

- o Uses the LGfL Net Sweeper filtering system, as a backup to the local proxy server.

- o Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;

- o 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;

- o Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

- o Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;

- o Informs all users that Internet/email use is monitored;

- o Informs staff and students that they must report any failure of the filtering systems directly to the ICT technician. Our ICT technician logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary;

- **Network management (user access, backup)**
  This school
  - o uses individual, audited log-ins for all users;

  - o uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services

  - o ensures the ICT technician is up-to-date with LGfL services and policies;

  - o 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 school's E-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 username and password for access to our school's network;

- we provide pupils with an individual network log-in username. From Reception they are also expected to use a personal password;

- all pupils have their own unique username and password which gives them access to the Internet and to the Learning Platform;

- we use Windows Server Active Directory for usernames and passwords;

- makes clear that no one should log on as another user and makes clear that pupils 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 pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

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

- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;

- 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.

- maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by the ICT technician; equipment installed and checked by approved Suppliers;

- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:

- 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;

- makes clear responsibilities for the daily back up of MIS and finance systems and other important files;

- uses secure data transfer; this includes 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);

- our wireless network has been secured to appropriate standards suitable for educational use;

- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

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 change their passwords twice a year

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail, and makes clear personal emails should be through a separate account.

- Uses Londonmail with students as this has email content control.

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses.

- 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 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.

Pupils:
- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.

- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.

- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.

- Year R/1 pupils are introduced to principles of e-mail through the Visual Mail facility in the London Learning platform or closed 'simulation' software.

- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home

Staff:
- Staff can only use the LA or LGfL e-mail systems on the school system

- Staff 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 pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX systems;

School website
- o The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- o Uploading of information is restricted to our website authorisers: e.g. Headteacher and ICT technician

- o The school web site complies with the statutory DfE guidelines for publications;

- o 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;

- o 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;

Learning platform

- o Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- o Photographs and videos uploaded to the schools Learning Platform will only be accessible by members of the school community;
- o In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform.

Social networking

Staff, Volunteers and Contractors
- Staff are instructed to always keep professional and private communication separate.
- 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.
- for the use of any school approved social networking will adhere to school's communications policy.

School staff will ensure that in private use:
- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:
- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:
- Parents are reminded about social networking risks, age restrictions and protocols
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- o We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation.

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

Strategic and operational practices

At this school:

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

- Staff are clear who are the key contact(s) for key school information are.

- 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

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed;

  o Staff;
  o Governors;
  o Pupils;
  o Parents.
  This makes clear staffs' responsibilities with regard to data security, passwords and access.

Technical Solutions

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

- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.

- We use RAv3 with its 2-factor authentication for remote access into our systems.

- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content

- We store any Protect and Restricted written material in a lockable storage area.

- Staff have secure area(s) on the network to store sensitive files.

- We require staff to log-out of systems when leaving their computer

- All servers are in lockable locations and managed by DBS-checked staff.

- We use grandfather-father-son tape backup scheme, for admin and curriculum servers. Tapes are taken off site at least weekly.

- 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 get a certificate of secure deletion for any server that once contained personal data.

- 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.

6. Equipment and Digital Content

Personal mobile phones and mobile devices
- Designated 'mobile use free' areas are situated in the setting. The areas which should be considered most vulnerable include: toilets and changing areas.

- 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 out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. 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 Head Teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Teacher 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. 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.

- Mobile phones and personally-owned mobile devices brought into 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.

- 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.

- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

- 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 e-safety 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.