ONLINE SAFETY (E-SAFETY) POLICY

	Name of School	Spring Grove Primary School
	Policy review Date	April 2019
	Date of next Review	April 2020
	Who reviewed this policy?	SLT and GB

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety <u>must</u> follow the school's safeguarding and child protection processes.

LGFL School Online Safety Policy

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT 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

ONLINE SAFETY (E-SAFETY) POLICY

- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices:

ONLINE SAFETY (E-SAFETY) POLICY

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 *Spring Grove Primary School* with respect to the use of IT-based technologies.

- Safeguard and protect the children and staff.

- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.

- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)

ONLINE SAFETY (E-SAFETY) POLICY

- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

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

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• 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, e.g. network manager
	• 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.
ICT/Online Safety Co-ordinator and DSL	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents
	• Promote an awareness and commitment to online safety throughout the school community

ONLINE SAFETY (E-SAFETY) POLICY

Role	Key Responsibilities
	• Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee 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 online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise 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 concerns.
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • 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.
ICT/Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician/ICT Leader	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - 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 • That they keep 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 • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher

ONLINE SAFETY (E-SAFETY) POLICY

Role	Key Responsibilities
	• To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	• 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(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • 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, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • 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 **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 line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually • 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 safe behaviours and good online safety practice when using digital technologies out of school and

ONLINE SAFETY (E-SAFETY) POLICY

Role	Key Responsibilities
	realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • to consult with the school if they have any concerns about their children's use of technology • 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 use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology 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.

ONLINE SAFETY (E-SAFETY) POLICY

Communication:

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

- Policy to be posted on the school website.

- Policy to be part of school induction pack for new staff.

- Regular updates and training on online safety for all staff.

- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.

- Staff and pupils are given information about infringements in use and possible sanctions.

- Online Safety Coordinator (ICT Leader) 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 online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- 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.

ONLINE SAFETY (E-SAFETY) POLICY

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the *Computing curriculum* and other curriculum areas as relevant. 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 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 the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- runs a rolling programme of online safety advice, guidance and training for parents, including:

  - All parents asked to sign Acceptable Use Agreements to ensure that the principles of online safety are made clear;

  - Suggestions for safe internet usage at home;

  - Demonstrations and practical session held at school;

  - Information provided through school newsletters and links to the school website.

ONLINE SAFETY (E-SAFETY) POLICY

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;

- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;

- understand the importance of adopting good online safety practice when using digital technologies in and out of school;

- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- 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.

ONLINE SAFETY (E-SAFETY) POLICY

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

- all members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) 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;

- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;

- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;

- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;

- has the educational filtered secure broadband connectivity through the LGfL;

- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). 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;

- ensures network health through use of Sophos anti-virus software (from LGfL);

- Uses DfE, LA or LGfL approved systems.

- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

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

ONLINE SAFETY (E-SAFETY) POLICY

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;

- 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;

- Has daily back-up of school data (admin and curriculum);

- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);

- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data 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 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.

- Pupils have their own unique username and password which gives them access to the Internet and other services (younger pupils use cohort logins);

- 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;

- 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 primarily to support their professional responsibilities.

- 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;

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

ONLINE SAFETY (E-SAFETY) POLICY

- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;

- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;

- This school 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. The school is GDPR compliant and has a DPO who will review this.

- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

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

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

- We require staff to use STRONG passwords.

E-mail

This school

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

- 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

- We use a number of LGfL-provided technologies to help protect users and systems in the school.

Pupils:

- We use the Db Primary pupil email system which is monitored by staff and limited to within the school community for pupil protection.

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

ONLINE SAFETY (E-SAFETY) POLICY

Staff:

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

- Staff will use LA or LGfL e-mail systems for professional purposes

- Use of external email accounts for professional purposes is prohibited.

- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- The school web site complies with statutory DFE requirements;

- 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;

- 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;

Cloud Environments

- Uploading of information on the schools' online learning space (Db Primary) is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;

- In school, pupils are only allowed to upload and publish within school approved 'Cloud' systems – Db Primary.

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 (Db Primary) for such communications.

ONLINE SAFETY (E-SAFETY) 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 and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

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

Strategic and operational practices

At this school:

- The school employs DPO from an external provider.

- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.

- 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 a single central record

ONLINE SAFETY (E-SAFETY) POLICY

Technical Solutions

- Staff have a shared drive on the network that is not accessible by pupils.

- We require staff to log-out of systems or lock down when leaving their computer.

- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.

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

- Details of all school-owned hardware will be recorded in a hardware inventory.

- Details of all school-owned software will be recorded in a software inventory.

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

- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

- We are using secure file deletion software.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & 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 and pupils are discouraged from bringing mobile devices into school.

- All pupil mobile devices will be switched off and handed in at reception on arrival at school. They must NOT be kept on the pupil's person; in their bag or personal tray during the school day.

- Personal mobile devices will not be used during lessons or formal school time.

- Staff members may use their phones only during school break times and mobile devices should not be accessible in the classroom during lessons. (Lockers are provided for phones and other belongings to be securely stored.)

- 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.

- All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any personal mobile device is prohibited.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

ONLINE SAFETY (E-SAFETY) POLICY

- If a student needs to contact his or her parents or carers, the school will contact them on the pupil's behalf. Parents are able to contact their child via the school office.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.

- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- School devices e.g. iPads must not be used to access personal accounts.

- PIN access to the device must always be known by the network manager.

Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school and any that are must be left with the main office during 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 but they must be left with the school's main office during the school day.

- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

- 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 – through the Online Safety aspects of the school's Computing Curriculum.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.

- Where contact with students, parents or carers is required, for instance for off-site activities staff will contact the school using their own device and the school will then contact the relevant party.

- 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.

- 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.

- 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 and then report the incident with the Headteacher / Designated Officer.

- If a member of staff breaches the school policy then disciplinary action may be taken.

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 (or annually).;

- 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, high profile use

- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;

- Pupils are taught about how images can be manipulated in their online 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 computing 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

For additional information see Appendix A7 - Cameras & Images Usage

Online Safety Policy - Appendix A - Cameras & Images Usage

Official use of Images/Videos of Children by the School

- All images taken by the school will be used in a manner respectful of GDPR. This means that images will be:

    o   fairly and lawfully processed

    o   processed for limited, specifically stated purposes only

    o   used in a way that is adequate, relevant and not excessive

    o   accurate and up to date

    o   kept on file for no longer than is necessary

    o   processed in line with an individual's legal rights

    o   kept securely

    o   adequately protected if transferred to other countries

- The Senior Leadership team is responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the school. This includes the management, implementation, monitoring and review of the School Image Use Policy.

- Written permission from parents or carers will be obtained before images/videos of children are electronically published by the school.

- Written parental consent will be sought to take and use photographs offsite for professional, marketing and training purposes. This may be in addition to parental permission sought for onsite images.

- Written consent from parents will be kept by the school where children's images are used for publicity purposes (such as brochures or publications), until the image is no longer in use.

- Parental permission will be sought on an agreed basis (include details e.g. annually, on admission to the school)

- A record of all consent details will be kept securely on file. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of and the record will be updated accordingly.

- Images will not be kept for longer than is to be considered necessary. A designated member of staff will ensure that all photographs are permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

- All images will remain on site at all times, unless prior explicit consent has been given by the Senior Leadership team and the parent or carer of any child or young person captured in any photograph. Should permission be given to take images off site, all relevant details are to be recorded, for example who, what, when and why and data will be kept securely (e.g. with appropriate encryption)

- The Senior Leadership team reserve the right to view any images taken and/or to withdraw or modify a member of staffs' authorisation to take or make images at any time.

- Any memory stick, CD or storage device containing images of children to be taken offsite for further work will be suitably encrypted and will be logged in and out by the Senior Leadership team and monitored to ensure it is returned within the expected time scale.

- Images or videos that include children will be selected carefully when used online and will not provide material that could be reused.

- Children's full names will not be used on the website in association with photographs.

- The school will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.

- Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.

- All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.

- Only official school owned equipment (e.g. work provided digital or video cameras) will be used by staff to capture images of children for official purposes. Use of personal cameras by staff is prohibited at all times.

- Any apps, websites or third party companies used to share, host or access children's images will be risk assessed prior to use. The school will ensure that images are held in accordance with the Data Protection Act and suitable child protection requirements (if necessary) are in place.

- Careful consideration is given before involving very young or vulnerable children when taking photos or recordings, who may be unable to question why or how activities are taking place.

- The school will discuss the use of images with children and young people in an age appropriate way.

- Images will not be taken of any child or young person against their wishes. A child or young person's right not to be photographed is to be respected.

- Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.

- Photographs will be disposed of should they no longer be required. They will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies will not to be taken of any images without relevant authority and consent from the Senior Leadership Team and the parent/carer.

Use of Photos/Videos by Parents/Carers

- Photographs taken by parents/carers at event/assemblies do not breach the data protection act as long as they are only for personal use.

- Digital video and images must not be shared on the internet such as Facebook, YouTube and other social network sites without specific consent from the parents of the children involved.

- Parents must make every attempt to only include their own child in photographs and videos taken at school.

- Parents/Carers are only permitted to take or make recording within designated areas of the school.

- The opportunity for parents/carers to take photographs and make videos can be reserved by the school on health and safety grounds.

- Parents and carers who are using photographic equipment must be mindful of others when making and taking images and should not take pictures of other parent's children unless given express permission by the child's parent.

- The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.

- Parents may contact the school's Senior Leadership team to discuss any concerns regarding the use of images.

Use of Photos/Videos by Children

- The school will discuss and agree age appropriate acceptable use rules with children regarding the appropriate use of cameras, such as places children cannot take the camera (e.g. unsupervised areas, toilets etc).

- The use of personal devices e.g. mobile phones, children's own digital cameras, is covered in the school Online -Safety policy.

- All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official for curriculum use.

- Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos.

- Photos taken by children for official use will only be taken with parental consent and will be processed in accordance with the Data Protection Act 1998.

- Photos taken by children for official use will be carefully controlled by the school and will be checked carefully before sharing online or via digital screens.

- Still and video cameras provided for use by children and the images themselves will not be removed from the school unless expressly permitted by the school's Senior Leadership Team (e.g. for a school trip/ sports event etc.)

Use of Images of Children by the Media

- Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's (or other relevant media) requirements can be met. A written agreement will be sought between parents and carers and the press which will request that a pre-agreed and accepted amount of personal information (e.g. first names only) can be published along with images and videos.

- The identity of any press representative will be verified and access will only be permitted where the event is planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.

- Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the school is to be considered to have acted in good faith.

Use of Professional Photographers

- Professional photographers who are engaged to record any events will be prepared to work according to the terms of the school's Online-Safety policy.

- Photographers will sign an agreement which ensures compliance with the Data Protection Act and that images will only be used for a specific purpose, subject to parental consent.

- Photographers will not have unsupervised access to children and young people.

Use of Closed-Circuit Television (CCTV)

- All areas which are covered by CCTV will be well signposted, and notifications are displayed so that individuals are advised before entering such vicinity.

- Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will generally be a maximum of 30 days. All recordings are to be erased before disposal.

- Regular auditing of any stored images will be undertaken by the Senior Leadership team or other member of staff as designated by the Senior Leadership team.

- If cameras record activities taking place on the premises which are of a criminal nature or give any cause for concern, then information will be referred to the appropriate agency.

- CCTV cameras will be appropriately placed within the school.

Use of Webcams

- Parental consent will be obtained before webcams will be used within the school environment for curriculum or educational purposes.

- All areas which are covered by webcams for security or safeguarding purposes will be well signposted, and notifications are displayed so that individuals are advised before entering such vicinity.

- Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will generally be a maximum of 30 days. All recordings are to be erased before disposal.

Parents Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:
  o the Internet at school
  o the school's chosen email system
  o the school's online managed learning environment <<name of system>>
  o IT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe and responsible use of the Internet, online services and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

This part of the agreement should be returned to school and will be kept on file.

The rest of this document should be kept by the parent/carer for their own reference.

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

Spring Grove Primary School rules for any external use of digital images are:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission.
e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and online media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- o **Common courtesy**
- o **Common decency**
- o **Common sense**

How do we show common courtesy online?
- o We ask someone's permission before uploading photographs, videos or any other information about them online.
- o We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?
- o We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is online-bullying** and may be harassment or libel.
- o When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?
- o We think before we click.
- o We think before we upload comments, photographs and videos.
- o We think before we download or forward any materials.
- o We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- o We make sure we understand changes in use of any web sites we use.
- o We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting abuse: thinkuknow.co.uk/parents/

LONDON GRID FOR LEARNING Appendix – C

Insert logo	Name of School	Spring Grove Primary School
	AUP review Date	April 2019
	Date of next Review	April 2020
	Who reviewed this AUP?	SLT and GB

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, **equipment and systems.**

Spring Grove Primary School regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

- I will not reveal my password(s) to anyone.

- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.

- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.

- I will not engage in any online activity that may compromise my professional responsibilities.

- I will only use the approved email system(s) for any school business.
  This is currently: [*LGfL StaffMail]*

- I will only use the approved *LGfL StaffMail and school approved communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business.

- I will not support or promote extremist organisations, messages or individuals.

- I will not give a voice or opportunity to extremist visitors with extremist views.

- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager / school named contact*.

- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

- I will follow the school's policy on use of mobile phones / devices at school and *will not take into classrooms / only use in staff areas.*

- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.

- I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.

- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.

- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will only access school resources remotely (such as from home) using the *LGfL / school approved system* and follow e-security protocols to interact with them.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I understand that GDPR require that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will alert a DSL if I feel the behaviour of any child may be a cause for concern.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to a DSL.

- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head / DSL*.

- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

- I will only use any LA system I have access to in accordance with their policies.

- I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ....Date..

Full Name .... (printed)

Job title / Role ....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature .... Date..

Full Name .... (printed)

LONDON GRID FOR LEARNING Appendix – D

Spring Grove Primary School -Key Stage 1: Acceptable Use Agreement

I keep **SAFE online** because …   ✓

I **CHECK** it's OK to use a website / game / app.

I **ASK** for help if I get lost online.

I **THINK** before I click on things.

I **KNOW** online people are really strangers.

I am **RESPONSIBLE** so never share private information.

I am **KIND** and polite online.

I **TELL** a trusted adult if I am worried about anything.

My trusted adults are:

Mum
Dad
Teacher

My name:

Date signed:

Spring Grove Primary School - KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- *I am an online digital learner* – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- *I am a secure online learner* - I keep my logins and passwords secret.
- *I am careful online* - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- *I am guarded online* - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- *I am cautious online* - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- *I am considerate online* - I do not get involved with bullying or sharing inappropriate material.
- *I am respectful online* – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- *I am responsible online* – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- *I am a creative digital learner online* - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- *I am a researcher online* - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- *I communicate and collaborate online* - with people I know and have met in real life or that a trusted adult has approved.
- *I am SMART online* - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement.

I know who are my trusted adults are and agree to the above.

Signed: Date:

_____   _____