Draft Online Safety Policy

October 2019

Headteacher's Signature:

Chair of Governor's Signature:

Date:

Review date: October 2022

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

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
   - 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 (separate documents):

A1: Acceptable Use Policy (Staff, Volunteers and Governors)
A2: Acceptable Use Policy (Pupils – adapted for phase)
A3: Acceptable Use Policy including photo/video permission (Parents)
A4: Photo permission form for students

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

Scope

This policy applies to all members of Seven Mills Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of Malmesbury Primary School

Roles and 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 the 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
- 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.

Designated Safeguarding Lead (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
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

- 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.

Computing curriculum Leader

To oversee the delivery of the online safety element of the Computing curriculum

Network manager/technician

- To report online safety related issues that come to their attention, to the computing leader
- 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 DSL/Headteacher
- 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 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 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 Policy with their child/children
- 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 Policy 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.

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.
- DSL acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to DSL 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).

Handling a sexting/nude selfie incident:

UKCCIS (UK Council For Child Internet Safety) "Sexting in schools and colleges" should be used.

This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL (Designated Safeguarding Lead). This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people When assessing the risks the following should be considered:
    - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
    - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
    - Are there any adults involved in the sharing of imagery?
    - What is the impact on the pupils involved?
    - Do the pupils involved have additional vulnerabilities?
    - Does the young person understand consent?
    - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

Animmediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13

5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

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.

2. Education and Curriculum Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE 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 Policy(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;
- ensures 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:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

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.

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 including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- 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.

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;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;

- 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. The same credentials are used to access the school's network / We also provide a different/use the same username and password for access to our school's network;
- 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:
- 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 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 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.

We require staff to change their passwords into the MIS, LGfL USO admin site, twice a year.

We require staff using critical systems to use two factor authentication.

E-mail

This school:

- Provides staff with an email account for their professional use, GMAIL 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, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use school Gmail pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the Gmail email systems on the school system
- Staff will use Gmail email systems for professional purposes
- 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 website 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 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 able to upload and publish within school approved 'Cloud' systems.

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 (see twitter 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 Policy.

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.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We 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

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- 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.

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be left securely in the office until the end of the day.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, 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.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- 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 personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- 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.
- 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.

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

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

The School strongly advises that student mobile phones and devices 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 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.

Phones and devices must not be taken into examinations. Students found in possession of a mobile device 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.

Staff use of personal devices

- Staff handheld devices, are allowed in school. 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 in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- 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.

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.

Appendix 1 Acceptable use policy for staff, governors and volunteers

What is an AUP?

We ask all children, young people and adults involved in the life of Seven Mills Primary to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Seven Mills Primary's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to the Designated Safeguarding Lead (DSL).

What am I agreeing to?

1. I have read and understood Seven Mills Primary's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).

3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.

4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

- not sharing other's images or details without permission
- refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.

8. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in Seven Mills Primary's social media policy/guidance.

9. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify [insert name/s] if I suspect a breach. I will not store school-related data on personal devices, storage or cloud

platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

10. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

11. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

12. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

13. I will follow the guidance in the Online Safety Policy for reporting incidents – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

14. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure 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: _____

Name: _____

Role: _____

Date: _____

To be completed by the Admin team

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 3 Parents acceptable internet use agreement

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my child access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- 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.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's online safety or online behaviour they will contact me.

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 include 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.
- I will not take and then share online, photographs of other children (or staff) at school events without permission.

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 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 use of the Internet and digital technology at home.
- I will inform the school if I have any concerns.

Childs name:_____

Parent carer signature:_____ Date:_____

Appendix 4 Photograph/Video Consent Form

We occasionally take photographs of the children at our school. These images may be used in our school prospectus, in other printed publications that we produce, on our school website, on project display boards in school, etc. We may also make video or webcam recordings for school-to-school conferences, examinations and coursework.

It is important that we protect your child's interests, respect your wishes and comply with Data Protection law. Please read the Conditions of Use below before answering the questions below and signing and dating this form. Please return the completed form (one for each child) to the school as soon as possible; we will not use a photograph or video of your child without consent.

Please note there are certain activities where we do not use consent as the basis for processing your child's data. There are described in our Privacy Notices. We may also take photos/video of your child for identification purposes and for evidencing their educational development – such data will sit on their file and not be shared unless the law requires us to do so or you have given your specific consent.

Where your child is over 13 years of age, we recommend that you complete this form with them, as children may be able to decide how their data may be used in certain circumstances.

Please note that you can withdraw your consent at any time. If you have any queries or wish to withdraw or review your consent, you can contact the school office.

Description of the use of Photographs or Images

Please circle appropriate response

May we use your child's photograph in the school hard-copy prospectus and other printed publications that we produce for promotional purposes? Please note: Printed publications are available to anyone	Yes	No
May we put your child's photograph and/or name on the school's website, including in online publications such as an on-line prospectus and other promotional material? Please note: Websites can be viewed throughout the world, not just the United Kingdom where UK law applies and, if copied from the website, images and information can no longer be controlled by the school	Yes	No

May we use your child's photograph and name on Social Media Please note: Social Media can be viewed throughout the world, not just the United Kingdom where UK law applies and if copied from Social Media, images and information can no longer be controlled by the school	Yes	No
May we record your child on video for Nativity play, internal school events, external school event and trips. Please note: this may include your child's voice as well as their image. Videos will only be made available to parents/guardians of the child	Yes	No

Conditions of Use

- This form is valid for the period of time your child attends the school, or if the child reaches the age of 13 and Parental Consent is no longer valid.
- The school will not re-use any photographs or recordings of your child that are incompatible with the original purposes explained to you
- If we use photographs of individual pupils, we will not use the full name of that child in any accompanying text or caption without consent, nor will we include any other personal data
- Parents should note that websites can be viewed throughout the world and not just in the United Kingdom (where UK law applies) and, when copied from the website, images and information can no longer be controlled by the school.

Further information on how we use your data and your child's personal data is in the Privacy Notice(s) available on our website or via the School Office

Name of Child	
Name of Parent/Carer:	
Signed:	
Date:	