DEVONSHIRE PRIMARY SCHOOL

ONLINE SAFETY POLICY

Key people/dates:

Designated Safeguarding Lead (DSL)	Mrs M Elsey
Online-safety lead	Mrs M Elsey
Online-safety / safeguarding link governor	Mrs E Catling
Computing subject lead	Miss R Byfield
PSHE/RSHE lead	Mrs S Sargeant and Mrs C King
Network manager / other technical support	Cygnet
Date this policy was reviewed and by whom	November 2025 by LL – amended link governor and PSHE/RSHE lead
Date of next review and by whom	November 2026 – ME/RB

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.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. Additionally, this policy has been written in line with 'Teaching Online Safety in Schools' 2019 as well as statutory RSHE guidance 2019.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate content on pupils' electronic devices, in line with the DfE's advice for schools on searching, screening and confiscation.

The policy also takes into account the National Curriculum computing programmes of study.

Aims:

This policy aims to:

- Set out expectations for all Devonshire community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline);
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform;
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to thrive online;
- Help our school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
        - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
        - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession;
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as our Behaviour Policy).

Scope

This policy applies to all members of the Devonshire community (including teaching and support staff, supply teachers, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

Devonshire Primary School is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The governing body (led by the online safety link governor)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board;
- Ask about how the school has reviewed protections for pupils in the home and remote learning procedures, rules and safeguards;

- Support the school in encouraging parents and the wider community to become engaged in online safety activities;
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings;
- Work with the Data Protection Officer (DPO), DSL and headteacher to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information;
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in our school;
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction;
- Ensure appropriate filters and appropriate monitoring systems are in place being aware that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding;
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

The Headteacher

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards; ● Foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding
- Oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported;
- Ensure that policies and procedures are followed by all staff;
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships;
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information; ● Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information;
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child safety first principles;
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles;
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident;
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised;
- Ensure that there is a system in place to monitor and support staff (e.g. network

manager) who carry out internal technical online-safety procedures;
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety;
- Ensure the school website meets statutory requirements.

The designated safeguarding lead (DSL)

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection [including online safety] … this lead responsibility should not be delegated" (KCSIE 2021)
- Work with the headteacher and technical staff to review protections for pupils in the home (the use of LGFL HomeProtect filtering for the home) and remote-learning procedures, rules and safeguards;
- Ensure "An effective approach to online safety that empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and the SENCOs) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies;
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns;
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply;
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information;
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training;
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors;
- Receive regular updates in online safety issues and legislation, be aware of local and school trends;
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life; ● Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents; ● Communicate regularly with the Senior Leadership Team (SLT) and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs (MyConcern) and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping; ● Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident;
- Staff are able to flag issues when not in school using My Concern The school's on-line

reporting system.

- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are also aware;
- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying;
- Facilitate training and advice for all staff, including supply teachers: ○ all staff must read KCSIE Part 1 and all those working with children Annex B ○ Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or Headteacher think it will provide a better basis for those staff to promote the welfare and safeguard children.
  - ○ it would also be advisable for all staff to be aware of Annex D (online safety)
  - ○ cascade knowledge of risks and opportunities throughout the organisation;

PSHE/RSHE subject leader

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ Relationships education, relationships and sex education (RSE) and health education curriculum;
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies;
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE;
- Ensure an RSHE policy is included on the school website;
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

The ICT technician is responsible for:

- As listed in the 'all staff' section, plus:
- Support the Headteacher and DSL team as they review protections for pupils in the home and remote-learning procedures, rules and safeguards;
- 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;
- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice;
- Work closely with the DSL/ DPO / LGfL nominated contact/ Computing subject leader to ensure that school systems and networks reflect school policy;

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.);
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Maintain up-to-date documentation of the school's online security and technical procedures;
- To report online-safety related issues that come to their attention in line with school policy;
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls;
- Monitor the use of school technology, online platforms and social media presence;

The computing subject leader is responsible for:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum;
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach;
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing;
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements. ● Collaborate with the DSL to regularly review the online safety policy.

Teachers

All teachers are responsible for:

- Teaching and embedding the computing and online safety curriculum as set out in the computing units of work;
- Supervising and guiding pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant);

All staff and volunteers

- Recognise that RSHE is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject; ● Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up;
- Know who the DSL is;
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education; ● Read and follow this policy in conjunction with the school's main safeguarding policy; ● Record online-safety incidents in the same way as any safeguarding incident and

report in the same way as any other safeguarding concern (MyConcern); ● Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself;

● Sign and follow the staff acceptable use policy and code of conduct/handbook; ● Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon;

- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils);
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place);
- When supporting pupils remotely, be mindful of additional safeguarding considerations;
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR;
- Be aware of security best-practice at all times, including password hygiene and phishing strategies;
- Prepare and check all online sources and resources before using;
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions;
- Notify the DSL of new trends and issues before they become a problem; ● Take a zero-tolerance approach to bullying and sexual harassment; ● Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – inform the DSL;
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues;
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Pupils

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually;
- Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen;
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher;

- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else;
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media;
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher;
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it;
- Consult with the school if they have any concerns about their children's and others' use of technology;
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers;
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns;
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

UK Safer Internet Centre:
https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Childnet International: http://www.childnet.com/parents-and-carers/hot-topics Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf Education programme from the National Crime Agency's CEOP Command
https://www.thinkuknow.co.uk/parents/

Educating pupils about online safety

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

Pupils are specifically taught about safe use of the internet. They will be taught what is acceptable and what is unacceptable, and what to do when they feel 'uncomfortable'.

As part of a broad and balanced curriculum all pupils are made aware of online risks and taught how to stay safe online. Assemblies, online safety themed days and guest speakers

may be used to educate pupils about the risks that can be encountered online. Pupils are taught about safeguarding issues, including how technology can provide a platform for issues such as child sexual exploitation, radicalisation and sexual predation.

Pupils are taught about the safe use of social media and, using age-appropriate resources, are taught how to stay safe from radicalisation, child sexual exploitation, FGM, grooming and peer-on-peer abuse. Pupils are equipped with the skills needed to stay safe and adopt safe online practices to help them recognise online risks and stay safe from abuse. We will ensure that key messages are shared in a way that is appropriate to children's needs, particularly for children with special educational needs or who are deemed vulnerable.

In **EYFS and Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private;
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable behaviour;
- Identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects, including in PSHE/RSHE, where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Handling online safety incidents and concerns

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RSHE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should talk to the DSL/ log a concern on My Concern to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding Policy
- Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy (if separate)
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school) or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL, through use of MyConcern, on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Sexting – sharing nudes and semi-nudes

We recognise the importance of following guidance on sexting and as such refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the DSL to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in KCSIE and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area. Any incidents should be referred to the DSL who will decide next steps and whether other agencies need to be involved.

Cyber-bullying
Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE/ RSHE education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with other agencies if it is deemed necessary to do so.

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in KCSIE and also a document in its own right.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff will work to foster a zero-tolerance culture. school will take all forms of sexual violence and harassment seriously using relevant guidance. KCSIE makes specific reference to behaviours such as bra-strap flicking and the careless use of language which will not be tolerated and incidents will be reported to the DSL.

Examining electronic devices

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or

could be, used to: cause harm, and/or disrupt teaching, and/or break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should: delete that material, or retain it as evidence (of a criminal offense or a breach of school discipline), and/or report it to the police.

Monitoring and Filtering

KCSIE obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At Devonshire Primary School, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. However, it is not possible to guarantee that unsuitable material will never appear on a terminal.

In school we monitor all pupil devices using ‘Classroom Cloud’. This System emails key personnel with details of inappropriate use of devices.

At home, school devices are filtered using LGFL HomeProtect when on home WiFi connections.

When pupils log into any school system on a personal device, activity will also be monitored here. For example, at Devonshire, we use G Suite for in person and remote learning and filters are applied whether the pupil or staff member is logging into a school Chromebook, a home Chromebook or into a chrome profile on a Windows laptop/ computer.

Email

- Pupils at this school use the LondonMail system from LGfL for all school emails
- Staff at this school use the StaffMail system for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. They have virus and malware scanning on every email, as well as ‘rude word’ checking, etc. Any emails found to exceed the threshold (set at ‘3’) are flagged up and reported to authorised users. Authorised users have the ability to look at any emails within both systems. Other webmail systems are blocked. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff. Where appropriate members of SLT may contact staff through their personal mobile phones. Staff should not contact parents using their personal Staffmail and parents should not try to contact staff through Staffmail. Instead, if a parent wishes to contact a member of staff, this must be done through the office email (office@devonshire.sutton.sch.uk). If a parent learns of a staff member's personal Staffmail address, this must be referred to the headteacher. Use of a different platform must be approved in advance by the DPO/ headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the

DSL (if by a child) or to the Headteacher (if by a staff member).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- All pupils and staff have a Google email address as this forms their Chrome login used to access the G Suite. However, pupils cannot access Gmail and therefore cannot send emails from this address. Staff can access their Gmail account but it is not actively used as a means for emailing and is discouraged.
- Staff or pupil personal data should never be sent/shared/stored on email.
  - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
  - Internally, staff should use the school network, including when working from home when remote access is available via the G Suite
  - When emailing information about a pupil and/ or their family, staff should use initials wherever possible.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for appropriate purposes only, or for the purpose of fulfilling the duties of an individual's role.

Pupils/students are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network and therefore, the G Suite on school devices in the school.

Home devices are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage can be tracked. The devices are with the LGfL HomeProtect home filtering software and are filtered even when on home wifi connections.

Volunteers, contractors, governors and parents have no access to the school network or wireless internet on personal devices.

More information is set out in the acceptable use agreements in the appendices.

Device usage

Staff and pupils are reminded those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring you own device Pupils

Only pupils, with permission to walk to or from school alone are able to have a mobile phone in school and in such cases parents must sign a mobile phone contract (appendix 5). If they choose to bring a mobile phone into school, it must be left with the class teacher for the duration of the school day. If the phone is used inappropriately, the pupil will not be able to bring the device into school again. It is the child's responsibility to hand their phone in to their class teacher. The school takes no responsibility for loss or theft. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Pupils will be able to use the school iPads to support their learning; they must do so in line with the pupil acceptable use agreement (appendices 2 and 3).

All staff

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Staff must not use personal mobile devices or cameras when pupils are present. Pupil/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they must inform the headteacher.

Volunteers, contractors, visitors and governors

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher and/ or the site manager should be sought and this should be done in the presence of a member staff.

Parents

Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 4.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

Trips/ events outside of school

For school trips/events away from school, teachers will be issued a school duty phone and this number will be used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher.

Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

How the school will respond to issues of misuse

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social Media

Devonshire Primary School's social media presence

Devonshire Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The website co-ordinator is responsible for managing our Twitter and Facebook social media accounts and checking our Wikipedia and Google reviews. They will follow the guidance in the LGfL / Safer Internet Centre online-reputation management document here.

Staff, pupils' and parents' social media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as

they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The school has an official Twitter and Facebook account (managed by Laura Love) but will not use this platform to respond to general enquiries. For this, parents' must contact the school directly, in person or through the school website. We also ask parents/carers not to use this channel to communicate about their children.

Email is the official electronic communication channel between parents and the school where parents can contact the school office email address. Parents are also able to ring the school office.

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions will not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Social media incidents

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Devonshire Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to the Assistant Headteacher responsible for the website. The site is managed by / hosted by [delete as appropriate; may be the same] [Insert names/companies here; NB LGfL schools receive web hosting at no extra cost]

Where other staff submit information for the website, they are asked to remember: ● The school has the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission;

- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published;
- Only images and videos of children whose parents/ carers have given permission for use can be used. Parents/ carers give individual permission for images/ videos published on the school website and images/ videos published on the school's Twitter account (see digital images and video).

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored Devonshire Primary School, no member of staff will use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network or the Google Drive in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing

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.

Pupils are advised to be very careful about placing any personal photos on social media. 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 / or a friend are subject to bullying or abuse.

Training

All new staff members will receive training on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

All staff members will be made aware of the following:

- Pupil attitudes and behaviours which may indicate that they are at risk of potential harm online;
- The procedure to follow when they have a concern regarding a pupil's online activity.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety in accordance with the school's safeguarding procedures. Any incidents will be logged on MyConcern in the same way as any other safeguarding issue.

This policy will be reviewed every two years by the computing subject leader. At every review, the policy will be shared with the governing body.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Acceptable Use Agreement (Parents/Carers)

At Devonshire Primary School, we ensure that all pupils have good access to digital technologies to support their learning and we expect all our pupils to agree to be responsible users in order to keep everyone safe.

Please read, discuss with your child and sign the acceptable use agreement that is relevant to their age (attached).

I understand that my child has received, or will receive, on line safety education to help them understand the importance of safe use of the technology and the internet – both in and out of school.

As the parents/carer of the pupil below, I understand that my child will have access to the internet and to ICT systems at school and is expected to follow the acceptable use agreement.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that pupils will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of material accessed on the internet and using mobile technologies.

I understand that the school takes inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. I understand that my child's activity on ICT systems will be monitored and that the school will contact me if they have concerns about possible breaches of the acceptable use agreement.

I understand that only children who have permission to walk home alone are able to have a mobile phone in school. If I choose for my child to bring a mobile phone into school, it must be left with the class teacher for the duration of the school day. I understand that it is my child's responsibility to hand their phone in to their class teacher and that the school takes no responsibility for loss or theft. I understand that before my child is able to bring their phone to school, I must complete a mobile phone contract.

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

I understand that if I take photographs or videos at school events that have other children or staff in them, I will not share these online or with the press.

Name of pupil:

Parent/carer name:

Parent/carer signature:

Date:

Appendix 2

Pupil Acceptable Use Agreement EYFS and Key Stage 1

This agreement will help keep me safe and help me to treat others respectfully.

Examples of how the children use mobile devices and computers include: i-pads for photos, interactive whiteboards and PCs to access educational games online, programmable toys to give instructions to and recordable microphones.

This is how I will keep safe online:

	Please tick each statement
I will only use the devices and websites my teacher says I'm allowed to use.	
I will check with a trusted adult before I use new sites, games or apps.	
I will remember that people online aren't always who they say they are and will not arrange to meet them.	
I won't send photos of myself or others.	
I won't share my personal information (including my name, address, telephone number, religion, ethnicity or health information).	
I will be kind and polite to people online and will not join in with bullying.	
I will tell a trusted adult if I am worried, scared or just not sure.	

Child's name:

Child's class :

Parent/Carer signature:

Date:

Appendix 3

Pupil Acceptable Use Agreement Key Stage 2

This agreement will help keep me safe and help me to treat others respectfully. In order to stay safe online I must remember:

I am an online digital learner – I will only use the school's internet and devices for school work and learning activities. I will only use sites, games and apps that trusted adults say that I can use.

I am secure online – I will not share my password with others or log in using someone else's details. I will not open any attachments in emails, or follow any links in emails, without first checking with a trusted adult.

I am private online – I will not give out my personal information (including my name, address, telephone number, my school name, religion, ethnicity or health information). I will never send photos of myself or others.

I am a rule follower online – I know that some websites and social networks have age restrictions and I respect this. I will not use the internet without a trusted adult being present or without their permissions, and will only visit sites that a trusted adult has agreed to.

I am respectful online – I will not post, make or share unkind, hurtful, rude or inappropriate messages or materials and will tell a trusted adult if I see these. I will not join in with cyber bullying or sharing of inappropriate material. I will not use inappropriate language when communicating online.

I am responsible online – I will tell a trusted adult if I find material or messages that might upset, distress or harm myself or others or if I find someone is being bullied online. I will not access or share inappropriate materials, websites, social networking sites or chat rooms.

I am careful online – I will not arrange to meet anyone offline. I understand that unless I have met someone in real life, I can't be sure who someone is online.

I understand if I breach the rules school may:

- Contact my parents;
- Contact the families of the affected children;
- Contact the police;
- Prevent me from using the internet and/or computing equipment in school;
- Remove my privilege of bringing my phone to school.

I will also take part in an online safety reflection session where I will discuss appropriate use of the internet and/or take part in additional learning activities based on the breach I took part in. My teacher will help me fill in a reflection sheet during the activity saying what I have learned about how to behave online in future.

I have read and understood this agreement.

Child's Name: Parent/Carer signature: Date:

Child's signature: Class

Appendix 4

Acceptable Use Agreement (staff, governors, volunteers and regular visitors)

When using the school's ICT system and accessing the internet in school, or outside school on a work device:

- I will not browse, access or attempt to access, inappropriate material, including but not limited to material of a violent, criminal or pornographic nature or material that is considered offensive or of an extremist nature by the school;
- I will not support or promote extremist organisations, messages or individuals;
- I will not use any improper language when communicating online, including in emails or other messaging services;
- I will not install any unauthorised software;
- I will not engage in any online activity that may compromise my professional responsibilities;
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this; ● I understand that I have a responsibility to ensure that I remain up to date and read and understand the school's most recent online safety and safeguarding policies.

Mobile device and camera safety

I have read and understand that:

- I must not use personal mobile devices or cameras when pupils are present, except with the Headteacher's consent;
- I may use my mobile phone on school premises when no pupils are present; ● I will use my professional judgement in extenuating circumstances; any use of a mobile device will have been agreed with a member of SLT;
- I may take a mobile phone on a school trip but they must only be used in emergencies and should not be used when pupils are present;
- Personal mobile devices cannot be used to take images or videos of pupils in any circumstances;
- Personal mobile devices cannot be used to take images or videos of staff, without the staffs' consent.
- The sending of inappropriate messages or images from mobile devices is prohibited;
- Photographs and videos of children will be carefully planned before any activity with particular regard to consent and adhering to the school's data protection policy; ● Photographs taken of children will adhere to the consents that the parents have given;
- I will report any concerns about another staff member's use of mobile phones to the designated safeguarding lead; and I will ask them to delete any images that I am aware have been taken;
- I will endeavour to ensure that no 3rd party takes a photo of the pupils;

- I will adhere to the online safety policy at all times.
- I will only use the school's ICT systems and internet for appropriate purposes or for the purposes of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit.
- I will let the computing subject leader or a designated safeguarding lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems responsibly, and, to the best of my ability, will ensure that pupils in my care do so too.

I understand that failure to follow the guidelines in the online safety Policy may be a breach of the School Disciplinary Procedures.

Name:

Signed:

Date:

Appendix 5

Devonshire Primary School

Devonshire Avenue, Sutton, Surrey, SM2 5JL
www.devonshireprimary.org

Email: office@devonshire.sutton.sch.uk Telephone – 020 8643 1174

Dear Families,

Walking Home Alone and Mobile Phones in Upper Key Stage 2

As you are aware, in Years 5 and 6, pupils are permitted to walk to and from school with the consent of their parents/carers.

Please be aware that this consent allows the children to walk home alone from school every day and they will be dismissed from the walking home door at the front of school.

Additionally, a number of requests have been made for children to be allowed mobile phones so that children can be contacted or make contact with others in the result of an emergency. Consequently, we have decided to allow this **only for Year 5 and 6 pupils, who walk home alone**, at your discretion. A simple phone that makes calls and texts is sufficient and they do not need to have the latest phone.

Pupils who have permission to walk alone and wish to be allowed access to their mobile phone must return the attached slip to their class teacher. If you wish for your child to walk home from school but not bring in a mobile phone, please leave the second section blank. Phones must be handed over to their class teacher as soon as they enter the classroom and will be returned to the children outside the school building as they are leaving the premises. During the school day, the phone will be turned off, locked away in a secure location and the owner will not have access to it.

We expect children to behave appropriately when walking home alone. If children do not meet our high expectations when walking home alone from school then the privilege may be revoked.

We would like to make it clear that under no circumstances should the children use their phones whilst on school premises (including the playground, front of school and other outdoor areas). If any pupil is found to be breaking these rules, or to have used their phone inappropriately, the phone will be confiscated immediately and this privilege will be removed. May we also remind pupils that in bringing their phone to school, they are solely responsible for looking after it and the school will not be held responsible for any loss/damage incurred.

Yours sincerely,

Upper KS2 Leader

Devonshire Primary School

Devonshire Avenue, Sutton, Surrey, SM2 5JL
www.devonshireprimary.org

Email: office@devonshire.sutton.sch.uk Telephone – 020 8643 1174 Walking

Home Alone in Year 5 & 6

I give permission for my child: Class:
to walk home alone from school.

Start Date: _____

Signed: Parent/Carer Please print your full name:

Date:

Mobile Phones being brought into school if children walk to or from

school Telephone number of phone being brought into school:

We agree to abide by the rules governing mobile phones in school and understand the consequences of breaking the rules. We understand that the school will not be held responsible for any loss/damage incurred.

I give permission for my child to bring a mobile phone to school **ONLY** on the days he/she walks home alone.

Signed: Parent/Carer Please print your full name:

Signed: Pupil

Date: