DEVONSHIRE PRIMARY SCHOOL

E-Safety Policy

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.

Aims

At Devonshire Primary School we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its safe and responsible use of technology;
- Establish clear mechanisms to identify and deal with incidents.

Legislation and guidance

This policy is based on the Department for Education'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.

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.

Roles and responsibilities

The governing body

The governor who oversees online safety is Dr Amin Mirza.

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4).

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

The DSL is responsible for:

- Working with the Headteacher, computing subject leader and other staff, as necessary, to address any online safety issues or incidents that have a child protection concern;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the Headteacher and/or governing body.

The ICT technician and computing subject leader

The ICT technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

The computing subject leader is responsible for:

- Monitoring online safety incidents logged on the online safety incident report log (appendix 6) and ensuring they are dealt with appropriately in line with this policy;
- Delivering staff training on online safety and ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Ensuring that online safety is embedded within the curriculum.

Teachers

All teachers are responsible for:

- Teaching and embedding the computing and e-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

All staff and volunteers will:

- Read, ensure they understand, sign and adhere to the school staff acceptable use agreement (appendix 4), and ensure that pupils follow the school's terms on acceptable use (appendix 2 and 3);

- Work with the DSL to ensure that any online safety incidents are logged on the online safety report log (appendix 6) and dealt with appropriately in line with this policy;
- Model safe, responsible and professional behaviours in their own use of technology.

Parents

Parents are expected to ensure their child has read, understood and agreed to the relevant pupil acceptable use agreement (appendices 2 and 3).

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

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, e-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 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.

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 personal, social, health and economic (PSHE) 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 external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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 offence or a breach of school discipline), and/or report it to the police.

Monitoring and Filtering

When pupils use the school's network to access the internet they are protected from inappropriate content by our filtering and monitoring systems. To minimise inappropriate use, pupils are supervised and guided carefully when engaged in learning activities involving online technology. Online safety education is embedded within the curriculum and pupils are taught how to use online technology safely and responsibly. The school will ensure that the use of filtering and monitoring systems does not cause 'over blocking' which may lead to unreasonable restrictions as to what pupils can be taught regarding online teaching. It is not possible to guarantee that unsuitable material will never appear on a terminal.

Email

All staff use LGFL's staffmail for email, and all pupils use LGFL's Londonmail for email. Both systems 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.

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.

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

Pupils using mobile devices in school

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 child 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. Pupils will be able to use the school i-pads to support their learning; they must do so in line with the pupil acceptable use agreement (appendices 2 and 3).

Staff use of mobile devices and cameras

- Staff must not use personal mobile devices or cameras when pupils are present;
- Staff may use mobile devices on school premises when no pupils are present;
- Staff will have their phones on them in emergency situations, this will be have been agreed by a member of SLT;
- Staff may take mobile phones on trips, but they must only be used in emergencies and should not be used when pupils are present.

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.

How the school will respond to issues of misuse

Clear processes are in place to identify and deal with incidents effectively. All pupils, parents and staff sign an acceptable use agreement.

Where a pupil misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident. We will follow the procedures set out in the behaviour policy and/or the following:

- Incidents will be reported to the Computing subject leader and DSL;
- An online safety incident log will be filled in and will contribute to developments in policy and practice in online safety within the school;
- Where pupils have breached the acceptable use agreement, they will fill in a pupil reflection sheet and may be asked to take part in a workshop to re-educate them about online safety and responsible use;
- Parents/carers will be informed of online safety incidents involving children for whom they are responsible;
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the appropriate authorities – police, Internet Watch Foundation, CEOP.

Incident forms are monitored by the computing subject leader and any learning points are used to develop staff training, pupil education or parent awareness e.g. specific lessons are taught relating to the breach; external speakers are invited to speak about specific topics; additional parent workshops are held for a particular year group etc.

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. An online incident report log can be found in appendix 6.

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.

Your child will be asked to read (or will have read to them) and sign an acceptable user agreement that is relevant to their age (appendix 2 or 3).

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 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: _____

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 e-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: _____

Class: _____

Date: _____

Appendix 4

Acceptable Use Agreement (staff, governors, volunteers and 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 for a violent, criminal or pornographic nature of 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 have a responsibility to 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 or staff in any circumstances;
- 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 been taken;
- I will endeavour to ensure that no 3rd party takes a photo of the pupils;
- I will adhere to the e-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 e-Safety Policy may be a breach of the School Disciplinary Procedures.

Name: _____

Signed: _____

Date: _____

Devonshire Primary School

Appendix 5

Email: office@devonshire.sutton.sch.uk

Telephone: 020 8643 1174

Dear Parents/Carers,

Walking Home Alone and Mobile Phones

Pupils are permitted to walk home alone from school with the consent of their parents/carers. 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 pupils, who walk home alone**, at your discretion.

Pupils who have permission to walk home 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 would like to make it clear that under no circumstances should the children use their phones whilst on school premises (including the playground and 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,

Mr James Wells

Upper KS2 Leader

Walking Home Alone

I give permission for my child:_____Class: _____

to walk home alone from school (please tick the relevant box/es)

Every Day ☐

or

Monday ☐

Tuesday ☐

Wednesday ☐

Thursday ☐

Friday ☐

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: _____

Online safety incident report log

Appendix 6

Online safety incident report log			
Date	List of children involved (notes kept under corresponding dates in green behaviour folder)	Logged on My Concern Y or n/a	Name and signature of staff member recording this incident