Stoneydelph Primary School

Online Safety Policy and Acceptable Use Agreements

Written by:	E. Parsons	**Date:**	June 2025
Date for review:	June 2027		
Approved by governors:	July 2025		

Stoneydelph Primary School

Online Safety Policy

Aims

Our school aims 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 use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE'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 images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

Roles and responsibilities

The School Standards Committee (SSC)

The SSC has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation.

The SSC will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Louise Turford.**

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 2)

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)

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT technical support and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Headteacher and/or governing board

This list is not intended to be exhaustive.

Technical Support Provider

The Local Authority technical support provider 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
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Ensuring that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet), and ensuring that pupils follow the school's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **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

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*

- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

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. (See also the school behaviour policy.)

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. Class teachers will discuss cyber-bullying with their class.

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 (see section 11 for more detail).

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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 (appendices 1-3). 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 educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is outlined in the Acceptable Use policy.

Pupils using mobile devices in school

Pupils may bring mobile devices into school where it is necessary for their safety e.g. for children walking home alone, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school.

Mobile phones must be handed in to the main office at the start of the school day where they will be stored safely until the child collects it at the end of their day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Alex Philips (Computing Lead) or Marc Wylie (Technical Support)

More information about staff use of devices- both school owned and personal- can be found in the Staff Code of Conduct.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, 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).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on My Concern. An example of the reporting form can be found in appendix 2.

This policy will be reviewed every 2 years by the headteacher . At every review, the policy will be shared with the School Standards Committee.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Anti-bullying
- Relational policy (behaviour)
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT acceptable use policy
- Social media policy

Appendix 1: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Stoneydelph Primary School

Acceptable Use Agreements

Written by:	E. Parsons	**Date:**	June 2025
Date for review:	June 2027		
Approved by governors:	July 2027		

Stoneydelph Primary School

Acceptable Use Policy

This policy incorporates all aspects of acceptable use relating to ICT and equipment within our school. It outlines the expectations for all stakeholders when using the systems provided by school making it clear the purpose of the use and the systems for reporting if something goes wrong.

These policies will be issued to the relevant parties on an annual basis in September. Staff will be expected to complete the agreement in Smartlog, the school's online Health and Safety compliance system. Volunteers, parents and children will be asked to complete either a MS Form or a paper copy of their understanding of the policies outlined below.

Staff and Volunteer Acceptable Use Policy

The review and maintenance of this policy is responsibility of the Executive Leadership Team of the Community Academies Trust.

Aim: The aim of this policy is to protect the school's IT systems and electronic data from damage (e.g. through introduction of viruses) and unauthorised disclosure through inappropriate staff and volunteer use.

Purpose: To set out protocols, procedures and restrictions for acceptable use of IT systems by staff and volunteers of the school.

Relationship to other policies: The Staff and Volunteer AUP is part of the school Online Safety Policy and also relates to Data Protection.

School Policy:
This Acceptable Use Policy reflects the school Online Safety Policy. The school will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for children and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy:
This Acceptable User Policy (AUP) applies to staff, volunteers and guests who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

User Responsibilities
I agree to:
- read, understand, sign and act in accordance with the School Online Safety policy
- complete the school's pink concern sheet to report any suspected misuse or problems to the Online Safety Leader (E.Parsons) and file copies within Online Safety concerns file.
- monitor ICT activity in lessons, extracurricular and extended school activities
- model the safe use ICT
- refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of the school or may bring the school into disrepute (this includes personal sites)

Education
- I understand that I am responsible for the Online Safety education of children
- I will respect copyright and educate the children to respect it as well

Training
- I understand that I will participate in Online Safety training

- I understand that it is my responsibility to request training if I identify gaps in my abilities

Online bullying
- I understand that the school has a zero tolerance of bullying. In this context online bullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures

Technical Infrastructure
I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures include:
- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media (unless I have permission)

Passwords
- I will only use the password(s) given to me
- I will never log another user onto the system using my login

Filtering
- I will not try to by-pass the filtering system used by the school
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately
- I understand that the school will monitor my use of computers and the internet

Data Protection
- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up.
- I will not carry data that uses personal information about anyone on an unprotected hard drive
- I will use the password protected external hard drive provided by school for all work related to school (teachers only)

Use of Images
- I will follow the school's policy on using digital images making sure that only those children whose parental permission has been given are published
- I will not use full names to identify people

Communication
I will be professional in all my communications and actions when using school ICT systems.

Email
- I will use the school provided email for all business matters
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media
- I will ask permission before I use social media with children or for other school related work

Personal publishing
- I will follow the Online Safety policy concerning the personal use of social media

Mobile Phones
- I will not use my personal mobile phone during contact time with children
- I will not use my personal mobile phone to contact children or parents with the exception of school trips where the Headteacher must be informed of their use.

Reporting incidents

- I will complete the school's pink concern sheet to report any suspected misuse or problems to the Online Safety Leader (E.Parsons)
- I will file copies within Online Safety Concerns File
- I will follow Child Protection procedures for all serious concerns
- I understand that in some cases the Police may need to be informed

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when children use ICT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

Acceptable Use Agreement

I have read, understood and agree to abide by the terms of the Acceptable Use Policy.

Name:……..…..

Position: …….

Signature:…… Date:……

Head signature:…… Date:…….

NB: Online signatures collected using Microsoft form

Laptop Acceptable Use Policy for Teaching Staff

Laptops are issued to staff based on a number of expectations. It is important to highlight these to avoid any confusion in the future.

- The laptops are owned and issued by the school and loaned to staff as and when they become available and at the discretion of the Headteacher. Loan of a laptop is not 'a right'.
- The school will maintain and pay for any failure of the machine of software as a result of normal use/wear and tear subject to costs and budget available.
- Laptops are issued primarily for the end benefit of the children and for staff to be able to support teaching and learning in a specific classroom or classrooms.
- Laptops are for use **only** by school employees.
- Staff laptops are not to be used directly by children who should use devices available in school.
- Laptops may be taken out of school and used at home. They must be carried in a proper laptop case to protect the computer during journeys. However, once off school property, it is expected that staff are responsible for the laptop. Any accidental damage, occurrence of theft etc occurring outside school property is the responsibility of the person loaned the laptop. (It is strongly advised that the laptop is insured by means such as ones own 'house hold insurance'. They may NOT be left in vehicles unattended)
- No additional software is to be uploaded to the school laptop
- Use of the Internet via the school lap top on/off site should always comply with the school's 'user agreement'/Online Safety policy.
- Since the laptop is to support children's learning; for periods of extended absence (i.e. 10 days or more) laptops are returned to school, unless an alternative arrangement has been made with the Headteacher.
- Following a period of loan, laptops should be returned to the school in condition they were given (less reasonable wear and tear).
- The laptop is loaned on the understanding that all due care and attention is taken over confidential information e.g. sensitive files are password protected or stored on a 'pen drive' which is kept securely.

Laptop Acceptable Use Agreement

I have read, understood and agree to abide by the terms of the Laptop Acceptable Use Policy.

Laptop Serial Number:……..

Laptop Asset Number:…….

Name:…….

Position: …….

Signature:…… Date:……

Headteacher :…… Date:…….

NB: Online signatures collected using Microsoft form

iPad Acceptable Use Policy for Teaching Staff

The aim of the Acceptable Use Policy (AUP) is to ensure that all staff are aware of their professional responsibilities in relation to iPads provided for staff use by the school. This AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, whilst the reputation of the school is maintained and the safety of all users is ensured. We expect staff to use their iPad in the classroom to enhance the teaching and learning experience for their pupils.

The iPads are to be used for professional purposes only and staff must bring their iPad to school every day, fully charged.

All users of the iPads will be required to review this AUP and sign the bottom of the form in order to demonstrate an understanding of these rules. iPad users will also agree to follow all relevant policies and procedures, be role models, display good practice and provide leadership in the use of these devices.

Teacher use of the iPad falls under the guidelines of Staffordshire Education Services' Acceptable Use Policy for technology. Access to the internet is monitored through our school's content filtering software and all rules and expectations are applied to the use of the iPad. All applications and documents stored on the iPad are the property of Stoneydelph School and are subject to regular review and monitoring.

Teachers will be provided with an iPad Air 2 (16GB), USB Cable, USB Charger and case. The iPad must be surrendered to Stoneydelph Primary School in appropriate working condition, immediately upon termination of employment or at the request of the Associate/ Executive Head. Stoneydelph Primary School reserves the right to require the return of an iPad from a staff member at any time and without notice.

At all times the iPad shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and email.

Individual users are responsible for the setting up of any home internet connection to use in conjunction with the iPad and no support will be provided for this by the school.

The following guidelines are general in nature as not every possible scenario can be thoroughly described or known at this point in time.

Maintenance and Care of Devices

- Staff issued with an iPad are expected to exercise the same care in respect of the security and upkeep of the iPad as if it were the employee's own property.
- Malfunctions or any other technical problems (either hardware or software related) should be reported immediately to the school's ICT technician via email, so that steps can be taken to have the problem rectified as quickly as possible. Under no circumstances is the employee to organise repairs to the iPad before reporting the problem.
- Lending the iPad to any third party is strictly prohibited. Use of an organisation-owned iPad by the user's friends and/or family is also strictly prohibited.
- Careless loss, damage or misuse of the iPad, its case or any other associated peripherals may result in disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.
- Users must keep the iPad away from food and drink at all times.

- The iPad screens are particularly sensitive to damage from excessive pressure on the screen. Users must avoid placing too much pressure and/or weight (such as folders and workbooks) on the screen in order to refrain from any unnecessary damage.
- The iPad must not be subjected to extreme heat or cold.
- Users must return the iPad to the correct tray in the iPad charging trolley when required for application synching and connect it to an available USB port.
- Users must keep the iPad clean and in good working order.

Security and Privacy

- It is a user's responsibility to keep their iPad safe and secure. When iPads are left unattended they must be locked in a secure cupboard in your classroom/school.
- It is a user's responsibility to ensure that their allocated iPad is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the iPad in a meeting room, any off-site venue and whilst travelling.
- iPads must not be left unattended or on view in motor vehicles at any time.
- If the iPad is lost, stolen or damaged, the Executive Head must be notified immediately. If necessary, the device will be remotely locked and/or wiped. Stoneydelph Primary School is not responsible for the loss of any personal files that may be deleted remotely from an iPad.
- The use of 'Jailbreaking' is strictly prohibited ('Jailbreaking' is the process which removes any limitations placed on the iPad by Apple, resulting in a less secure device).
- Users are required to set up a pin or pass code/password lock to keep the device protected. This code is strictly confidential and must not be divulged to staff or pupils.
- If you have enabled the facility on your iPad to receive and send school emails, you must ensure your iPad has a pass code/password lock in place.
- Along with the Acceptable Use Policy, staff must adhere at all times to the Data Protection Act (2018), The Computer Misuse Act (1990) and the school's health and safety policy when using iPads in school.
- In order to prevent access to confidential information, staff iPads should never be used by pupils.
- Users may not use private emails to send content that, if intercepted, would place the school in violation of laws or regulations.
- Staff may not use the internet to view illegal or inappropriate material that would place the member of staff or school at legal risk.

Applications

- Selected applications installed on staff iPads must align with educational purposes. Purchase and installation of such apps must be made through the Associate Head.
- Individual members of staff are also allowed to purchase appropriate apps for themselves, using their own Apple ID, as long as they are in keeping with the school's Acceptable Use Policy. The cost of such apps will not be reimbursed.
- Apps which would benefit other members of staff can be requested via email to the Associate Head, who will be responsible for the app budget.
- Staff should be aware that the school, via its web management system, can see what apps are installed on each iPad.
- Where apps are required to be deployed to all staff iPads simultaneously, the devices will need to be returned to the school iPad trolley for synchronisation.
- Updates to applications can be carried out by teaching staff, when required.
- Memory space is limited and academic content takes precedence over personal files and apps.

Social Media

- For the purposes of this policy, social media includes (but is not limited to) internet forums, blogs, wikis, podcasts, photograph websites (Flickr, Instagram, etc.), Facebook and Twitter. Staff should follow these guidelines in relation to any social media applications that they use, both in work and in their personal lives.

- Users should not access social media applications from the school's iPads when working in school unless it is for educational purposes, and is previously agreed and sanctioned by the Associate Head.
- Users should understand that anything they write (regardless of privacy settings) could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.

Use of Digital and Video Images

- Staff using iPads must be aware of the risks associated with sharing images and videos on the internet.
- Users must make good judgment when using the iPad camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Staff must not take, use, share, publish or distribute images of others without their permission.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Leadership team.
- Inappropriate media may not be used as a screensaver or background photo.
- Deletion of photos and videos may happen periodically by the Head of School or if a device's memory is full.

iPad Acceptable Use Policy for Teaching Staff

I have read, understood and agree to abide by the terms of the iPad Acceptable Use Policy.

iPad Serial Number:……....

iPad Asset Number:……....

Name:……..…..

Position: …….

Signature:…… Date:……

Associate Head signature:…… Date:…….

NB: Online signatures collected using Microsoft form

Parent and Carer Acceptable Use Policy

The review and maintenance of this policy is the responsibility of the Executive Leadership Team of the Community Academies Trust..

Aim: The aim of this policy is to provide parents and children with a common understanding of procedures to safeguard the children through appropriate, effective and safe use of the Internet and use of mobile devices.

Purpose:
- To set out for what purposes the Internet will be used in school
- To state the rules for child use of the Internet and mobile phones in school
- To state what will happen if these rules are broken.

Relationship to other policies: The Parent and Carer Acceptable Use Policy is part of the school Online Safety Policy and also relates to Data Protection.

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet.
The Internet will be used within school to support children's learning both formally (within taught lessons) and informally (outside taught lessons), at the discretion of a member of staff who will set guidelines and rules for its use. Children will be taught to be critical in their use of Internet sites.

Children may have opportunities to communicate with others through eSchools and blogs. This will only take place in accordance with the school's policy and procedure, so their full name will never appear online. Responsible and considerate language will be used at all times in communicating with others.

Children will:
- only use the school ICT systems for those activities which they have been given permission to use and under the appropriate supervision of a member of staff.
- use the Internet within the school to support learning..
- be made aware of what online bullying is and what to do if it happens.
- only use the user names and passwords they have been given
- not download and use material or copy and paste content which is copyright or not covered by the school copyright licenses.
- not attempt to search for, view, upload or download any material that is likely to be unsuitable in a school or is blocked by the schools filter.
- inform a member of staff if they have accidentally accessed inappropriate content.
- use responsible and considerate language in communicating with others.
- be encouraged to maintain a balance between the use of ICT and other activities.
- be encouraged to discuss their use of the Internet and those sites that are age specific especially Social Network sites.
- only use mobile phones when directed by staff.
- be encouraged to talk with their parents or carers about the rules for the safe use of the Internet (SMART)
- be made aware that the school may investigate incidents that happen outside of school but could have an effect on the school.

Failure to comply with these rules will result in one or more of the following:
- A ban, temporary or permanent, on the use of the Internet at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate restrictions placed on future access to school facilities.

If you do not understand any part of this document, you should ask a member of staff for guidance.

If you have any concerns regarding this policy, the form below must be completed, signed and returned to the school for our records.

Parent's name:	
Child's name	
School:	
Class:	
Date:	
Comments:	

NB: Online parent signatures collected using Microsoft form at the start of each academic year

Children's Acceptable Use Policy

Technology is a fantastic resource to support learning within school and to communicate with others. The School encourages its appropriate, effective and safe use. All users of technology and devices in school must agree to certain rules and will only use the equipment and software as instructed.

My Responsibilities

- I understand that I have rights and responsibilities in using ICT and will act responsibly when using technology, computers or the internet.
- I will learn the school's SMART rules to keep myself safe inside and outside of school
- I will report any suspected misuse or problems to a teacher or trusted adult within school.
- I will make sure there is permission to use any material that I find i.e. copyright

Communication – eSchools, email, social networks, blog etc.

- I will be careful in my communications making sure that nothing I write is offensive, and that it is considerate.
- I will not write anything that could be seen as insulting to the school.

Online bullying

- I understand that the school will not accept bullying in any form.
- I will be careful with all communications making sure that anything I write is considerate and could not be interpreted as bullying.
- I understand that I should report any incidents of bullying and know how to do this.

Children's Acceptable Use Agreement

I have read, understood and agree to abide by the terms of the Acceptable Use Policy.

Name:……..…..

School and Class:……..

Signature:…… Date:……

Teacher signature:…… Date:……

(please complete and return this form to the school office)

Device Loan Agreement for Stoneydelph Primary School

There may be occasions where devices need to be loaned to families, such as COVID 19, to support parents with Home Learning, Stoneydelph Primary has agreed to provide an electronic device to support access to online learning from home.

Parent/Guardian/Carer Agreement

As a parent/guardian/carer of a student, whom an electronic school device has been loaned, you have read and agreed to the following terms and conditions:

- The equipment provided is the property of Stoneydelph Primary School and is for the **sole use of assisting online learning** at home during school closure.
- I agree to ensure that:
  - Any user treats the equipment with appropriate care and the device is maintained in a good condition.
  - The device is always kept in its case.
  - The equipment is not left unattended without being stored securely.
  - Any user avoids food and drink near the device.
- I agree to ensure that any user only uses software licensed by the school, authorised by the school's ICT staff and installed by the school's ICT staff. I will not download any software or applications onto the device.
- Should any faults occur with the hardware or software, I agree to notify the school as soon as possible so that they may undertake any necessary repairs. I will not attempt to fix suspected hardware or software faults.
- I agree and understand that the school will not be able to provide technical support relating to home Internet connectivity.
- I agree that any broadband charges incurred by any user accessing the internet from any site other than school premises are not chargeable to the school.
- I will ensure that any internet access using the device at home is for an appropriate educational purpose.
- I confirm that I have read and agree to adhere to current school policies regarding the following: Online Safety, Social Media, Child Protection and Health and Safety.
- I agree that it is my responsibility to ensure my child follows the terms and conditions as set out above.
- I will return the device to Stoneydelph Primary School at the end of the period of home learning.

Replacements

Any theft must be reported to the police within 24 hours, a crime reference number should be obtained, and this must then be provided to Stoneydelph via the office. If stolen or damaged from a pupil's home, school would first ask for a claim under the user's household policy. Claims from the school will only be made if this is unsuccessful.

The school reserves the right not to replace a lost or damaged device.

Parent/Guardian/Carer Agreement:

I have read and agree the terms and conditions as set out above.

Name of Parent/Guardian/Carer: …….

Signature: …….

Date: …….

Loan Authorised by: …….

Date: ……

Device:

Serial Number: ……

Asset Number: ……

Please return the device to Stoneydelph Primary at the end of the period of home learning.