The Avenue Infant School

ONLINE SAFETY POLICY

(INCLUDING ACCEPTABLE USE POLICIES)

Adopted:

Signed on behalf of the Governing Body: Mr Stewart Miller

Position: Chair of Governors

Date: 7th December 2022

Review date: December 2022

Contents

1. 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. 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:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships education and health education
- 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.

PREVENT In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained via: Prevent- home office - https://www.elearning.prevent.homeoffice.gov.uk/edu/screen1.html This responsibility extends to online safety and protecting children from extremist material online.

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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) or deputy designated safeguarding lead (DDSL)/online safety lead. The governors who oversees online safety and are appointed online safety governor are Emma Russel and Alex Young.

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 5)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The role of the online safety governor will include:

- Regular meetings with Online Safety Lead & DSL/DDSLs
- Monitoring of online safety incident logs
- Monitoring of filtering checks & reports
- Reporting to relevant governors, boards and committee meeting

3.2 The headteacher

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

3.3 The designated safeguarding lead, deputy safeguarding leads & online safety lead

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding leads (DDSLs), including the DDSL responsible for online safety, are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DDSL responsible for online safety is the Deputy Headteacher: Jamie Pell.

The DSL takes overall responsibility for the safeguarding and safety for the members of the school community, including online safety, however DDSL responsible for online safety lead takes the lead for online safety in school working closely within and with the safeguarding team.

The DDSL with responsibility for online safety takes the lead responsibility for online safety, with the support of the wider safeguarding team, 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 manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Keeping a running log of online safety including: actions, incidents, parental information support/interactions and filtering systems checks (appendix 7)
- Ensuring that any online safety incidents are logged (see appendix 1/7) 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/safeguarding policy/Anti-bullying policy
- Updating and delivering staff training on online safety
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring the filtering system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Reviewing security checks & filtering and monitoring system reports on a daily basis (sent daily via email)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 ICT technical support contractors

The ICT manager is responsible for:

- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that users may only access the network and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Ensuring that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply
- Ensuring the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Ensuring that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher and online safety lead for investigation / action / sanction
- Ensuring that monitoring software / systems are implemented and updated as agreed in school policies
- 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

That the following is implemented:

- Internet access is filtered for all users. We use an educational filtered system that prevents unauthorized access to illegal websites. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident; whichever is sooner. The DSL/DDSLs and IT support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the headteacher.
- Email Filtering: We use mail filtering software that prevents any infected email to be sent from or received by the school. Infected is defined as: an email that contains a virus or script (i.e malware) that could be damaging or destructive to data; spam email such as a phishing message.
- Encryption: All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are to be encrypted. Any loss or theft of device such as laptop is to be brought to the attention of the head teacher immediately. The head teacher will liaise with the online safety governor to ascertain whether a report needs to be made to the Information Commissioner's Office.

- Passwords: All staff will be unable to access a device that can access personal or confidential data without a unique username and password.

3.5 All staff and volunteers

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

- 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 3)
- Working with the DSL/DDSL to ensure that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy & the safeguarding and child protection policy
- Ensuring all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensuring they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Ensuring that in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy & the safeguarding and child protection policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the 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 sign on behalf of the pupils, where appropriate) (appendices 3)
- Ensure they had read and signed the parents Acceptable Use Policy (appendix 4)

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 resource sheet – Childnet International

3.7 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 5).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of our curriculum offer and this is embedded across and throughout our broad and balanced curriculum. Teaching pupils to stay safe online and keeping children safe online in school is a crucial part of our online safety approach within the curriculum. Our approach to online safety runs through every aspect of our work with children, including (but not limited to):

- Curriculum planning, including Relationships education and health education & computing
- CPD for staff to develop our online safety curriculum
- Safety assemblies throughout each term
- Parental support and engagement

At The Avenue Infant School we will offer and believe that (see appendix 8):

- A planned online safety curriculum should be provided as part of computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Curriculum coverage: 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

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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access, where appropriate
- Updates on areas emerging around online safety at a local or national level
- Information in simply guides, taken from NOP, for parents relevant to age & stage of pupils on our social media platforms

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

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is, at an age appropriate level, 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. 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/DDSLs will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7. 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 2/3/4/5). 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 set out in the acceptable use agreements in appendices 2/3/4/5 and the misuse policy in appendix 7.

8. 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing 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 (see appendix 7).

9. 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 policy in appendix 7. 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 and in line with the misuse policy in appendix 7. 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.

10. 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL/DDSLs 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.

11. Monitoring arrangements

The DSL/DDSL logs behaviour and safeguarding issues related to online safety. The online safety report log can be found in appendix 8.

This policy will be reviewed every year by the DDSL with responsibility for online safety: Jamie Pell. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly (360 review with Computing Lead).

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Code of conduct
- Data protection policy and privacy notices

The Avenue Infant School The Avenue, Wellingborough, Northants, NN8 4ET 01933 276366	THE AVENUE INFANT SCHOOL **Online safety Incident Log**	The Avenue Infant School The Avenue, Wellingborough, Northants, NN8 4ET 01933 276366

Online safety Lead Teacher Online safety Lead Governor	Jamie Pell Emma Russel	
Details of Online safety Incident		
Type of incident	Bullying or harassment	
	Cyberbullying or harassment	
	Sexting (self-taken indecent images)	
	Deliberately bypassing security or access	
	Hacking or virus propagation	
	Racist, sexist, homophobic, religious hate material	
	Terrorist material	
	Sexual images/ pornography	
	Other (Please specify) ……	
Date of Incident		
Time of Incident		
Where the incident occurred		
Name of person reporting the incident		
Who was involved in the incident	Child/ young person	
	Staff member	
	Other (Please specify)	

Description of the incident		
Nature of the incident	Accidental	
	Deliberate	
Did the incident involve material being…	Created	
	Viewed	
	Printed	
	Shown to others	
	Transmitted to others	
	Distributed	
	Harassment	

Could this incident be considered as…	Grooming	
	Cyberbullying	
	Sexting (self taken indecent imagery)	
	Breach of acceptable use policy	
	Other (please specify) ……	
Action Taken	Staff	
	Incident reported to head/ senior leader	
	Child involved (if necessary)	
	Parents informed	
	Disciplinary action taken (please specify)	
	Child debriefed	
	Senior leader/ Online safety Lead	
	Advice sought from children's social care	
	Incident reported to police	
	Incident reported to CEOP	
	Incident reported to Internet Watch Foundation	
	Incident reported to IT services	
	Online safety policy to be reviewed/ amended	

Outcome of incident/ investigation

Children's Social Care		
Police/ CEOP		
School		
Individual staff member/ child		
Parents		
Other (HR/ Legal etc)		

Learning from the case

Key Learning Point 1	
Key Learning Point 2	
Key Learning Point 3	

Recommendations and Timescales

Recommendation 1		Timescale to be implemented	
Recommendation 2		Timescale to be implemented	
Recommendation 3		Timescale to be implemented	

THE AVENUE INFANT SCHOOL

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupil's learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. This includes not allowing anyone else at home to use school ICT systems without agreement from the headteacher.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers **using official school systems**. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school or profession into disrepute.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school

- When I use my mobile devices (laptops / mobile technologies) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not deliberately upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not deliberately use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. Any inadvertent breach of this will be reported to the Online safety Lead.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- **Social networking** is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

I understand that I am responsible for my actions in and out of the *school:*

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

APPENDIX 3

Please share this with your child and ask them to sign at the bottom/ sign for them to show that they understand and will follow these rules.

THE AVENUE INFANT SCHOOL

Acceptable Use Policy – Pupils

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school equipment for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences to my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

APPENDIX 4

THE AVENUE INFANT SCHOOL

Parent / Carer Acceptable Use Agreement

Name of Child **Class**

Digital technologies have become important to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that children will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

We will try to ensure that children will have good access to digital technologies to enhance their learning and will, in return, expect the children to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents are aware of the school expectations of the children in their care and children will need to sign/ adults sign on their behalf to indicate that they are aware of the school rules for safe internet and technology use. Parents are requested to sign the permission form below at different points to show their support of the school in this important aspect of the school's work.

INTERNET USE

PLEASE NOTE: The school's ICT system & virus protection are updated and reviewed regularly. Pupil's computers are on a different network to the school's administration system. A high level filtering system is in operation on the school's network which only allows access to websites suitable for primary aged children.

RULES FOR RESPONSIBLE INTERNET USE

★ When children are accessing the internet they will be supervised by an adult.
★ Pupils will not be issued with individual email accounts (until Year 2 when separate permission will be sought) but may have opportunity to use a group/class email address under direct supervision.
★ Pupils will only visit websites that an adult has given them permission to do so.
★ Pupils will be advised that if they see anything that they are unhappy with, they will tell an adult immediately.

1. I have read and understood the school rules for responsible internet use and give permission for my child to access the internet.
2. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.
3. I agree that the school cannot be held responsible for the nature or content of materials accessed through the Internet and mobile technologies.
4. I agree that the school is not liable for any damages arising from use of the Internet facilities where all reasonable precautions have been taken.
5. I will discuss the school's acceptable use policy for children with my child and I will encourage my child to adopt safe use of the internet and digital technologies at home. I will inform the school if I have concerns over my child's online safety.

I give permission for my child to access the internet whilst in school.

Signed

The use of social networking and on-line media

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

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

*How do we show **common courtesy** online?*

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

*How do we show **common decency** online?*

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

*How do we show **common sense** online?*

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

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

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

I agree to follow the guidelines for use of social media as outlined above and understand that there will be appropriate action taken by the school should any inappropriate behaviour which impacts upon the school or any member of the school community be drawn to their attention.

Signed

In order to support those parents who may be less familiar with use of the internet we have listed a variety of additional measures that you could take at home to support your child's safe use of the internet in the 'online safety' part of our school website. You can also find our online safety questionnaire and policy on there.

Alternatively, speak to your child's class teacher or Mr Pell our online safety lead, about any support that you would like or suggestions that you might have.

APPENDIX 5 Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use personal devices that I've brought into school for activities that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name _____ Signed _____

Date _____

APPENDIX 6 **Online Safety Log – Incidents/Information Sharing/Filtering**

DATE:	ACTIVITY:	ACTION/OUTCOMES:

APPENDIX 7

The ICT Misuse Policy

1. Aim

The ICT (Information and Communication Technology) Misuse Policy aims to ensure that any allegation, which is made in respect of intentional or unintentional misuse of any online technologies, is addressed in a responsible and calm manner. This includes any known or suspected breaches of the acceptable use policy, camera and image policy, internet policy and mobile phone policy.

Allegations must be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT misuse policy should also outline the sanctions that are applied if an incident occurs.
The overall priority should be to ensure the safety and wellbeing of children and young people at all times. If it is suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the safeguarding policy and procedures should be implemented with immediate effect. These procedures should also be followed if an allegation of abuse is made against any employee, manager, volunteer or student. The safeguarding policy should take precedence over all others and referrals should be made to the appropriate agency as deemed necessary.

2. Scope

The ICT misuse policy applies to all individuals who have access to and/or are users of work related ICT systems. This includes children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.
The policy should be implemented in respect of any potential breaches of the acceptable use policy, camera and image policy, internet policy and mobile phone policy.

3. Responsibilities

The registered person and the senior designated person for safeguarding are responsible for ensuring that the procedures outlined in this policy are followed. These procedures should be followed if an allegation of misuse is made against a child, young person or adult.

4. Policy Statement

Clear and well-publicised policies and procedures which will influence practice are the simplest and most effective way for the safe use of ICT to be upheld. Such policies and procedure should ensure the promotion of acceptable use and clearly define those behaviours which are not. The sanctions to be imposed in respect of any incidents of misuse should be identified.
It is important that:

- Relevant online safety policies and procedures are fully implemented, monitored and reviewed. These policies and procedures should be rigorous, manageable and reflective of practice and should be shared with all ICT users. The senior designated person for safeguarding is responsible for the management of such policies.
- All ICT users should be made aware of possible signs of potential misuse. Adults, in particular, are responsible for observing practice and behaviours, so that any significant changes in such are identified at the earliest opportunity.
- All ICT users should be made aware that the misuse of ICT and/or breaches of relevant policies and procedures are taken seriously, and that potential sanctions could be applied, should such concerns be raised.
- Effective reporting and whistle-blowing procedures should be in place and promoted.

It should be acknowledged, however, that no system or procedure can be considered completely safe, secure and fool-proof. It should therefore be accepted that the potential for ICT to be misused, whether intentionally or unintentionally will remain. The aim of the online safety policies is therefore to minimise such opportunities and risk.

5. Procedures

General

All incidents should be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions put in place.

The context, intention and impact of each incident should determine the response and actions to be taken. This allows a degree of flexibility in the application of sanctions. For example, a series of minor incidents by one individual is likely to be treated differently than a one-off occurrence; similarly unintentional and intentional access to inappropriate websites will instigate different levels of intervention and sanctions.
All online safety incidents should be recorded and monitored, and any potential patterns in behaviours identified, to enable such issues to be addressed proactively and for protection to be afforded.
All incidents
The following procedure should be followed for all incidents.

- The incident should be reported to the senior designated person for safeguarding. A written incident record should be made, and the situation monitored.
- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident may be escalated to a 'serious' level.
- If the incident relates to the inadvertent access to an inappropriate website, it should be added to the banned or restricted list and filters should be applied, where relevant.
- In respect of misuse by children and young people, parents and carers must be informed of the alleged incident and should be advised of any actions to be taken as a result.
- Sanctions should be applied in accordance with the acceptable use policy.

There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is unsuitable in a childcare environment and should be acted on.

Reporting
An open reporting policy should be in place which means that all inadvertent breaches and access to inappropriate materials are reported. The non-reporting of such breaches should result in the concern being escalated.

Serious Incidents
All serious incidents must be dealt with promptly and reported to the senior designated person for safeguarding and the registered person immediately.
The context, intention and impact of the alleged misuse must be considered.
Appropriate actions should be agreed between the senior designated person for safeguarding and the registered person.
All details should be accurately and legibly recorded. The reason why any decision is made should also be noted.
If at any stage a child or young person is or has been subject to abuse of any form, the safeguarding policy should be implemented with immediate effect. A referral should be made through Northamptonshire County Council protection procedures or through children's social care and the police, where applicable.
If the incident relates to an allegation made against an employee, manager, volunteer or student; and there is a suggestion that a child or young person has been subject to any form of abuse, the safeguarding policy will again be implemented with immediate effect. The local authority designated officer must be contacted in the first instance in respect of any allegation made against an adult. The police and Ofsted must also be contacted.
No internal investigation or interviews should be carried out in respect of any allegations, unless explicitly requested otherwise by an investigating agency.
If allegations of abuse are made, children's social care, the police and/or the Local Authority designated officer will be the investigative bodies. It must therefore be ensured that no action is taken which could compromise any such investigations.
Where applicable, any hardware implicated in any potential investigations of misuse should be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.
Internal disciplinary procedures should not be undertaken until investigations by the relevant agencies have been completed. Legal or human resources advice should be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.
On completion of both internal and external investigations, or sooner where appropriate, an online safety review should be undertaken and policies and procedures amended and updated as necessary. A consultation on any proposed revisions should be held with all ICT users as appropriate. Revised policies and procedures should be circulated as applicable.

By nature, serious incidents most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment through the use of portable media devices such as mobile phones, or grooming. These incidents may be instigated by a child, young person or adult.

The following incidents must always be reported to the police, SWCPP, children's social care, Local authority designated officer and Ofsted.

- Discovery of indecent images of children and young people.
- Behaviour considered to be 'grooming'.
- Sending of obscene materials.

By not reporting such incidents, an offence may be committed.

The seriousness of such allegations should be fully recognised, and all such incidents must be reported to the police immediately. No attempt should be made to download, print or send any materials found. Further offences could be committed by doing so.

If potentially illegal material is discovered, as far as is reasonable practical, the equipment or materials found should not be touched. Computers or other devices should not be switched off unless authorised to do so by the police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer remains on).

6. **Illegal material and activities which must be reported to the Internet Watch Foundation**

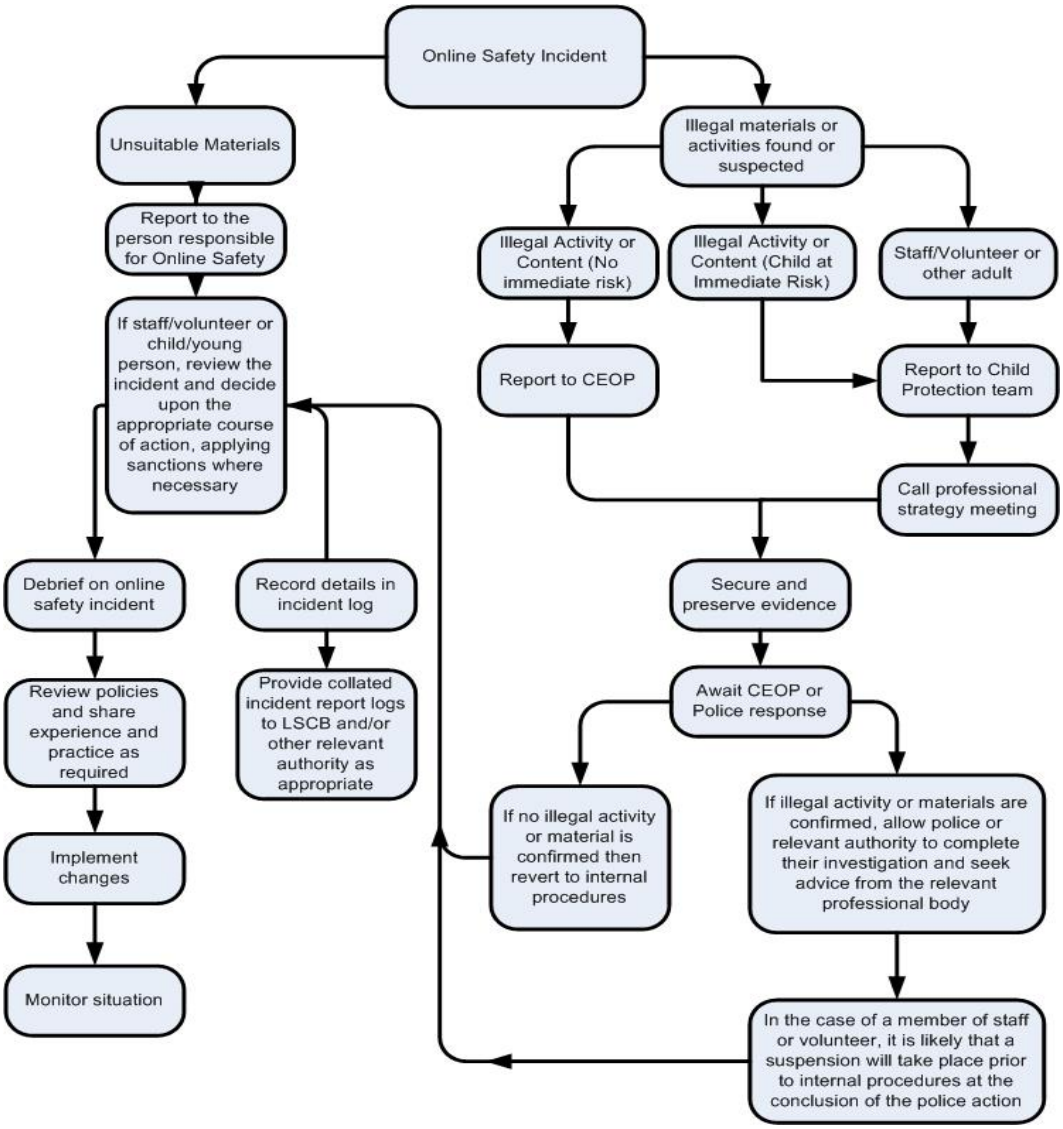
   A report should also be made to the Internet Watch Foundation – Homepage | Internet Watch Foundation (iwf.org.uk) If potentially illegal materials, including images of child abuse have been accessed online, giving details of the website address. If it is unclear whether the content is illegal or not, the concern should be reported as a matter of caution.

7. **Media attention**

   If a serious incident occurs, it may attract intense media interest and speculation. On such occasions, every possible attempt should be made to ensure that children and young people, parents and carers are protected and supported appropriately.

   An agreed media strategy should be implemented, and statements only released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern should be the safeguarding and welfare of the children, young people and their families. Advice should be taken from services for children and young people where appropriate before any media engagement is undertaken.

8. **Responding to incidents of misuse- Illegal Incidents**



9. Authorisation and review

Agreed by:……..

Authorised signatory:……

Date:……..

Date of review:……

ICT Online-Safety programme showing progression from EYFS through KS1, including whole school activities -

Whole school	• Safer Internet day Notes/Information in newsletters to support parents • Regular updates sent to parents with useful links and information • Our school website with supportive documents and information for parents • Age restrictions – using technology safely and respectfully -Gaming and online gaming. • Online-Safety guidelines shared with visitors • Online safety posters displayed around school –SMART • The benefits of rationing time online • Use of suggested search engines for research projects – e.g. Kiddle. Kiddle.co Wacky Safe. KidRex. ... Safe Search Kids • Responsive to e-safety concerns should they arise • E-safety poster referred to and children reminded of our E-safety
Reception	• Instructions to stay on certain programs during certain lessons • Importance of sharing and supporting each other when using ICT • Asking for adult support when stuck - Identifying a trusted adult to tell when something goes wrong • Basic rules of using technology – ipads/laptops. • Introduce e-safety poster. • Buddy the dog's internet safety story. • Think you know – https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/ (Episode 1)
	SCARF – PSHE Scheme • Know age-appropriate ways to stay safe online. • Share ideas about activities that are safe to do on electronic devices. • What to do and who to talk to if they feel unsafe online.
Year 1	• Sharing worries with an adult • Circle time discussions on using the internet at home safely • Penguin Pig story • Use of the internet as part of ICT lessons • Use of ICT for playing games ie online maths resources.
	Purple Mash Below is introduced in Autumn 1. Continue throughout year at start of lessons/new topics. • Children can log in to Purple Mash using their own login. • To login safely. • To understand the importance of logging out when they have finished. • Use of personal passwords and importance of keeping this safe - What is personal information? How do I keep it private? • Think about private and personal information and protecting this. • To create an avatar and to understand what this is and how it is used.
	• SCARF – PSHE Scheme Think you know – https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/ (Episode 2) • Basic rules to keep safe online, including what is meant by personal information and what should be kept private; the importance of telling a trusted adult if they come across something that scares them. • That sometimes people may behave differently online, including by pretending to be someone they are not • About how the internet and digital devices can be used safely to find things out and to communicate with others – Spring 1: Geography To find out about animal habitats • About the role of the internet in everyday life • That not all information seen online is true.

Year 2	• Always sharing concerns with adults • Use of personal passwords and importance of keeping this safe and not sharing it with others • How to deal with pop ups
	Purple Mash Below is introduced in Autumn 1 and is continued throughout the year at the start of lessons. • To know how to refine searches using the Search tool. • To know how to share work electronically using the display boards. • To use digital technology to share work on Purple Mash to communicate and connect with others locally. • To have some knowledge and understanding about sharing more globally on the Internet. • To introduce Email as a communication tool using 2Respond simulations. • To understand how we talk to others when they aren't there in front of us. • To open and send simple online communications in the form of email. • To understand that information put online leaves a digital footprint or trail. • To begin to think critically about the information they leave online. • To identify the steps that can be taken to keep personal data and hardware secure. • Chicken Clicking story • Digiducks Big Decision story • Think you know website - Lee and Kim
	SCARF – PSHE Scheme Think you know - https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/ (Episode 3) • Basic rules to keep safe online, including what is meant by personal information and what should be kept private; the importance of telling a trusted adult if they come across something that scares them. • That sometimes people may behave differently online, including by pretending to be someone they are not. • About how the internet and digital devices can be used safely to find things out and to communicate with others. • About the role of the internet in everyday life • That not all information seen online is true.