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: 3rd December 2025

Review date: December 2026

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
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

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, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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

2.1 General KCSIE 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 and sex education (RSE) and health education - GOV.UK
- Searching, screening and confiscation
- Generative AI: product safety expectations - GOV.UK

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.

2.2. 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.

2.3 Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "overblock".

KCSIE 2025, states the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring (see section 3 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via Helen Morrall or Natalie De La Salle and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at https://safefiltering.lgfl.net and training is provided for all staff / safeguarding teams / technical teams as appropriate.

At The Avenue Infant School:

- web filtering is provided by Securly on school site and for school devices used in the home
- changes can be made by Easi PC, via Helen Morrall or Natalie De La Salle
- overall responsibility is held by the DSL, with further SLT support from the online safety lead
- technical support and advice, setup and configuration are from Easi PC
- regular checks are made weekly by Natalie De La Salle to ensure filtering is still active and functioning everywhere. These are evidenced on the LGfL log
- an annual review is carried out – *latest review October 2025*

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices. At The Avenue Infant School we:

- use physical monitoring by staff watching screens of users
- have a filtering system on all devices including iPads
- monitor the use of both student and adult devices to ensure safety for all online activity

3. Roles and responsibilities

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Helen Morrall
Deputy Designated Safeguarding Lead responsible for filtering and monitoring	Natalie De La Salle
Deputy Designated Safeguarding Leads	Natalie De La Salle Louise Lucas Jodie Halford
Link governor for safeguarding	Bob Ballard Parul Bhagat
Curriculum leads with relevance to online safeguarding and their role	Natalie De La Salle – online safety, PSHE Katie Mason – Computing
Technical support contractors	Easi PC
Appropriate Filtering Provider	Securly

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 governor who oversees online safety and are appointed online safety governor are Bob Ballard and Parul Bhagat.

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 lead/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: Natalie De La Salle.

The DSL takes overall responsibility for the safeguarding and safety for the members of the school community, including online safety and understanding the filtering and monitoring systems and processes in place, however the DDSL responsible for online safety lead takes the lead for online safety in school, working closely within and with the 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- 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 6)
- Ensuring that any online safety incidents are logged (see appendix 1/6) 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
- Work alongside the DSL and Easi PC to ensure an appropriate level of security protection procedures, such as filtering and monitoring systems, are in place and 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 weekly, monthly and annual basis, and responding to any alerts emailed via our filtering provider (Securly)
- 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
- Undergoing at least annual training in online safety to ensure the most up to date issues can be addressed

This list is not intended to be exhaustive.

3.4 ICT technical support contractors

The ICT technical support contractor, alongside the DSL and DDSL 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

- Ensuring that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply
- Ensuring that 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 filtering system (Securly) that prevents unauthorized access to illegal websites. Illegal content (child sexual abuse images). Securly is a member of the Internet Watch Foundation CAIC list and ensure that all users are blocked access to to IWF CAIC list of domains and URLs. 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)
- Ensure they keep themselves informed about potential online risks and harms by keeping up to date with online safety bulletins provided in the newsletter/social media updates

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

4.1 Curriculum

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 relationships and sex education and health education - statutory guidance.pdf & National Curriculum - Computing key stages 1 to 2
- 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, in an age appropriate manner, 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

Lessons children receive, while at the Avenue will support them gain skills and knowledge around online safety to enable them meet their end of primary school standards listed below.

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 some photos, sounds and videos have been created with Artificial Intelligence (AI) and are not always real
- 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

5.1 Educating parents

The school will raise parents' awareness of internet safety in letters or other communications home, in information via our website, curriculum activities, parents' evenings, parent online safety information sessions 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 (i.e. via half-termly learning newsletters)
- Updates on areas emerging around online safety at a local or national level
- Information in simple 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.

5.2 Social Media

As stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

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

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). We ask parents to respect age ratings on gaming and social media platforms wherever possible and not encourage or condone underage use. It is worth noting that clear legal duties are set out in the Online Safety Act - GOV.UK including stringent age assurance to protect children in online activity.

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

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

Although the school has an official Facebook and X-Twitter account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and The Avenue Images Statement. The Images Statement clearly explains the reasons and uses for taking any images of children and how they will be used. Parents/carers

are asked to write to the school if there is any reason from a safeguarding perspective their child may not be included in images used for social media purposes.

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

Commented [GU1]: We have an Images statement which is sent to parents and parents have to opt out in writing so this statement may need rewording to reflect this.

Commented [ND2R1]: Amended.

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 e-safety lessons within the computing curriculum, 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.

6.3 Examining electronic devices

Children at The Avenue are not permitted to bring electronic devices into school this includes tablets, phones and smart watches. As such, any electronic devices on children's person or in found in bags will be confiscated and retained in the office securely, until then end of the day when they can be returned directly to the adult collecting the child. The DSL or any DDSL's can carry out a search on children's bags or person if they have reasonable grounds for suspecting a child may have brought an electronic device into school.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation
- Notify the parent at the end of the day

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Avenue recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Avenue will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

7.1 Acceptable use

All pupils, parents, staff, volunteers and governors are expected to digitally sign an annual agreement which includes 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 and 5.

7.2 School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Allison Munns.

The site is hosted by E4education.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

7.3 Social Media

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

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

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

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

Allison Munns is responsible for managing our X-Twitter and Facebook accounts.

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and The Avenue Images Statement clearly explains the reasons and uses for taking any images of children and how they will be used. Parents/carers are asked to write to the school if there is any reason from a safeguarding perspective their child may not be included in images used for social media purposes.

Commented [GU3]: We have an Images statement which is sent to parents and parents have to opt out in writing so this statement may need rewording to reflect this.

Commented [ND4R3]: Amended.

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

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
- Ensure that the anti-virus and anti-spyware software are updated, with any risks actioned
- Keeping operating systems up to date by always installing the latest updates
- Contacting Easi PC if there are any concerns over the security of the device

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.

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 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. 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 6.

This policy will be reviewed every year by the DDSL with responsibility for online safety: Natalie De La Salle. At every review, the policy will be shared with the governing board. The review will be supported by an annual audit and risk assessment (LGfL tool) 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

APPENDIX 1 – Online safety Incident Log

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	Natalie De La Salle Bob Ballard and Parul Bhagat	
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	
Could this incident be considered as…	Harassment	
	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	

APPENDIX 2 – Staff Acceptable Use Policy

THE AVENUE INFANT SCHOOL

Acceptable Use Policy – Staff/ Volunteers

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.

Staff read and sign an annual declaration to agree these terms.

For volunteers only:

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.

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.

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.
Parents are requested to sign the permission in the form below at different points to show their support of the school in this important aspect of the school's work.

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 questionnaire and policy on there. Alternatively, speak to your child's class teacher or our online safety lead about any support that you would like or suggestions that you might have.

INTERNET USE

PLEASE NOTE: The school's ICT system, including filtering and monitoring, & 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 and this system is routinely checked and reviewed.

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 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 e-safety.
6. I agree to follow the **guidelines for use of social media** as outlined below 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.

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**

As stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

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

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). We ask parents to respect age ratings on gaming and social media platforms wherever possible and not encourage or condone underage use. It is worth noting that clear legal duties are set out in the Online Safety Act - GOV.UK including stringent age assurance to protect children in online activity.

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

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

Although the school has an official Facebook and X-Twitter account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

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.

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 a member of the senior leadership team, 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.

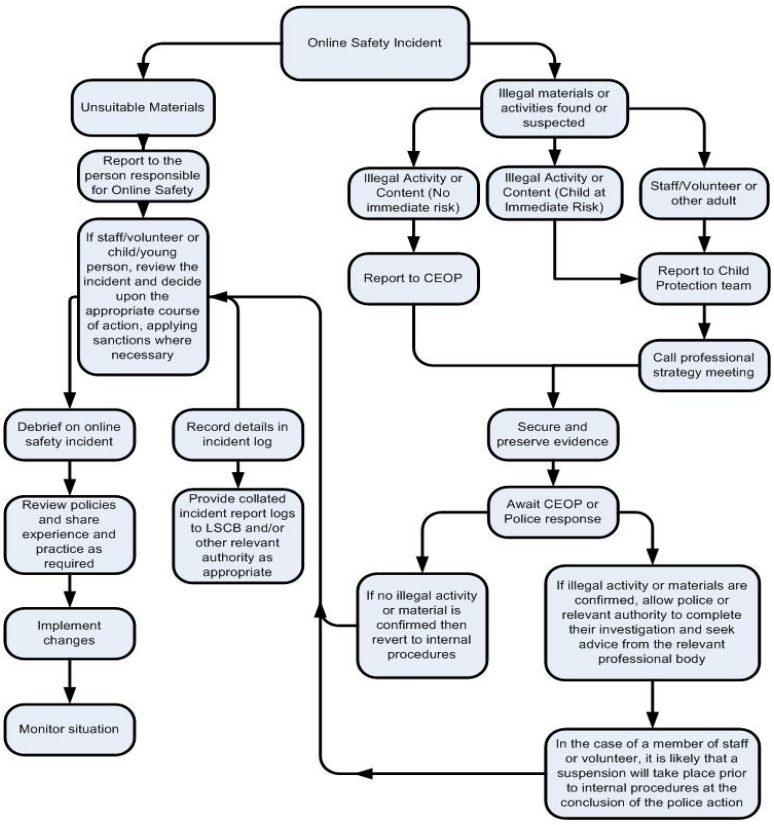
Name | Signed

Date

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

DATE:	ACTIVITY:	ACTION/OUTCOMES:

APPENDIX 7


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Computing Online-Safety Curriculum

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.