Digital Safety Policy

Digital Safety Policy (Including EYFS)

Policy Review Date: September 2025
Reviewed By: J Callaway, SLT & Board of Governors
Next Review: September 2026 (or following incident, legislation or interim guidance)

September 2025 Reviewed & ratified by:

Headteacher: Mrs J Callaway

Chair of Governors: Dr Catherine Kidd :

This policy is available on the school website and up on request.

Updates and Amendments to Policy

Date	Section Heading	Update Details	Page N°
28/01/2019	4) Pupils Evaluation of Internet content	If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Coordinator. i. The Computer Coordinator must then complete an incident section in the 'Online Safety Log'. ii. The Computer Coordinator will review the incident and take appropriate course of action. This may include adjusting filtering, reviewing policies, asking for assistance from Pro-Networks, sharing experience with staff and/or parents/carers and applying sanctions. iii. The incident will be reported to the SLT. If staff or pupils discover Illegal material the Computing Coordinator and Designated Safety Lead must be informed immediately. i. Procedures will be followed as above when discovering unsuitable sites. ii. If a child is at risk procedures will be followed according to the 'Safeguarding Children and Chid Protection Policy' and 'Keeping Children Safe in Education Part 1' iii. The incident will also be reported to CEOPs.	6
28/01/2019	5) Management of e-mail	pupils must immediately tell a teacher if they receive offensive e-mail. The teacher must then report it to the Computing Coordinator who must complete an incident section in the 'Online Safety Log' and review the incident as stated in section 4);	6
28/01/2019	Appendix 2	Incident sheet from Online Safety Log	11
11/3/2020	2.2 How the Internet benefits education.	Access to educational online programs.	5
15/9/2022	Significant review	Updating of all areas	
20/11/2024	Throughout	Changed from online safety to digital safety to recognise that there are digital risks offline too.	3, 5, 6, 7, 8, 9, 12, 13
20/11/2024	Rational	Updated rationale	4
21/11/2024	Parents	Resource links updated	7
20/11/2024	Educating pupils about digital safety	Changes made to more accurately reflect the national guidance	8
September 2025		All updates shown highlighted in Yellow	

CONTENTS

This policy applies all staff, volunteers and pupils in the School, including in the EYFS & Wraparound.

Computing Coordinator: Mrs Jones
Designated Safeguarding Lead: Mrs Joanna Callaway (Headteacher)

RATIONALE

The world has become an increasingly digital place, with greater and greater use of technology in all sectors of society, filtering into the home, workplace, leisure and education. Avalon School firmly believes in the educational benefits of the use of technology, including curriculum internet use, particularly as these skills are vital to access life-long learning and for future employment. In delivering the curriculum, teachers will make use of technology such as interactive whiteboards, desktop computers, laptops, digital cameras, iPads, and a range of programs, apps and web-based resources.

However, most technologies present risks as well as benefits. It is essential that children are safeguarded both online and offline from inappropriate and potentially harmful sources. The 4 key categories of risk are content, contact, conduct and commerce (these will be discussed in greater detail below). Whilst online safety is a large part of digital safety, it is also recognised that there can still be risks when using digital technology that is not connected to the internet.

At Avalon, we aim to have an effective whole school approach to digital safety that empowers us to protect and educate our pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Good planning and monitoring that recognises the digital safety risks, will help to ensure appropriate, effective and safe pupil use. Use of technology, including the use of the internet will be planned, task-orientated and educational within an environment that uses effective filtering and is well monitored. It is recognised that directed and successful use of technology will also reduce the opportunities for activities of dubious worth. Whilst unmediated access brings with it the possibility placing of pupils in embarrassing, inappropriate and even dangerous situations.

At the same time, it is important the pupils aren't restricted too much or denied access altogether for fear of technology and / or the risks. Pupils need to learn to recognise and avoid these risks and need to know how to cope if they do come across inappropriate material.

Similarly, we recognise that it is important that parents and carers adopt strategies for the responsible and safe use of technology. Therefore, we also aim to educate and raise awareness of digital safety in the wider community too.

Digital safety depends on staff, governors, advisers, visitors, parents/carers and, where appropriate, the pupils themselves taking responsibility for the use of technology and associated communication technologies.

Please also read in conjunction with the following policies (not exhaustive list) that further reinforce Avalon's Digital Safety policy:

Acceptable use of IT policy
Child protection and safeguarding policy
Anti-bullying policy
PSCHEE policy
Mobile phone and camera policy
Staff code of conduct
Low Level Concerns policy

1. Aims

Our school aims to:

- Have robust processes in place to ensure the digital safety of pupils, staff, volunteers and governors
- Deliver an effective approach to digital 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 digital 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, misinformation, disinformation 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

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

DfE 'Filtering and monitoring standards for schools and colleges'

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

Online Safety Act 2023

DfE 'Generative artificial intelligence in education'

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 digital safety, and monitor digital safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy and training is updated regularly.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that digital safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including digital 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
- review the effectiveness of filtering and monitoring provision at least annually
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.

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

Details of the school's designated safeguarding lead (DSL/ DDSL) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the staff in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Computing lead and other staff, as necessary, to address any digital safety issues or incidents.
- Liaise with the SENCO and be alert to the specific needs of children with special educational needs and disabilities (SEND) and understand the additional risks they face online.
- Managing all digital safety issues and incidents in line with the school child protection policy
- Ensuring that any digital safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on digital safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on digital safety in school to the headteacher and/or governing board
- knowledge and skills (including training) are updated at least annually
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

This list is not intended to be exhaustive.

3.4 The ICT management system

In conjunction with Obsidian Networks, the school is responsible for:

- 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 that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any digital safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- A filtering and monitoring review is conducted at least annually to assess effectiveness

This list is not intended to be exhaustive.

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 and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any digital safety incidents are logged and dealt with appropriately in line with this policy (see Appendix 2)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour 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'
- Low Level Concerns, including Digital Low Level Concerns must be reported to the DSL and recorded and managed in accordance with the school's Low Level Concerns Policy, KCSIE 2025 and the Staff Code of Conduct.
- Staff receive regular updates and training at least annually.

This list is not intended to be exhaustive.

Whole School Approach

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL will liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

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 can seek further guidance on keeping children safe when using digital technology from the following organisations and websites:

UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/what-are-the-issues

Thinkuknow: https://www.ceopeducation.co.uk/professionals/guidance/thinkuknow-parents-and-carers/

Wirral Safeguarding: https://www.wirralsafeguarding.co.uk/online-safety-guidance-parents/

Childnet: https://www.childnet.com/help-and-advice/parents-and-carers

https://www.childnet.com/resources/parents-and-carers-resource-sheet/

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.

4. Educating pupils about digital safety

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

The text below is taken from the National Curriculum Computing programmes of study. (P.179)

In **Key Stage 1**, pupils should be taught to:

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

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

- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Furthermore, the guidance on relationships education, relationships and sex education (RSE) and health education also states:

progression in the content [should] reflect the different and escalating risks that young people face as they get older. This includes how to use technology safely, responsibly, respectfully and securely, how to keep personal information private, and where to go for help and support. (p.39)

By the **end of primary school**, pupils should know (p.22 and 33):

- 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.
- That bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing.
- Where and how to seek support (including recognising the triggers for seeking support), including whom in school they should speak to if they are worried about their own or someone else's mental wellbeing or ability to control their emotions (including issues arising online).
- That for most people the internet is an integral part of life and has many benefits.
- About the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Why social media, some computer games and online gaming, for example, are age restricted.
- That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- Where and how to report concerns and get support with issues online.

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

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

All schools have to teach Relationships education and health education in primary schools.

5. Educating parents about digital safety

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

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 in Computing lessons as part of the termly Curriculum Overviews.

- Who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to digital safety, these should be raised in the first instance with the headteacher (DSL)

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Health, Citizenship, Economic Education (PSHCEE), and other subjects where appropriate.

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

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

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

The DSL will 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

The headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff.
- 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 cooperation

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the headteacher should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher (DSL) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

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 (appendix 1). 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.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

More information is set out in the acceptable use agreements in appendix 1

8. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs

The headteacher and Obsidian Networks (IT Service Support Provider) will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. IT support (Obsidian) will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, Obsidian and the DSL will conduct a risk assessment.

Deliberate breaches of the filtering system will be reported to the DSL, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Staff Code of Conduct

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

9. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and Obsidian Networks, and

manages concerns in accordance with relevant policies depending on their nature, such as . the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

All concerns, discussions and decisions made, and the reasons for those decisions, must be recorded in writing

Appendix 1 – Acceptable Computer Use Policy, included in the Safeguarding booklet, sent out to Parent/Carers each academic year.

As part of your child's curriculum and the development of Computing skills, Avalon School provides supervised access to the Internet. We believe that the use of the World Wide Web and Email is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Acceptable Computer Use Policy and talk about them with your child as appropriate to their age. Then sign consent form so that your child may use the Internet at School.

We take positive steps to deal with this any risk of the children in our School having access to undesirable materials, including our Internet provider operating a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Our rules also concern the types of communications that children make using computers and other technology. We would like your support in helping to ensure that the children at the School are using technology in a responsible and polite manner and never in a way that could upset another person or spoil their work.

A full copy of our digital policy is on the School website or available in School should you require a copy.

Should you wish to discuss any aspect of Internet use please contact Mrs Jones, our Computing Coordinator, or you child's class teacher in the first instance.

Please read and discuss with your child then sign and return to the School.

- Children must ask permission before accessing the Internet.
- We expect all children to be responsible for their own behaviour on the Internet, just as they are anywhere else in School. This includes materials they choose to access, and language they use.
- Children must only use websites and search engines as directed by staff.
- Children are expected not to use any rude language in their email communications and contact only people the staff have approved.
- Children should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc, memory drives etc. may be brought in to School and used without approval from staff first.
- Children not complying with these expectations will be warned, and subsequently, may be denied access to Internet resources.

Digital Safety and the Internet

Nursery, Pre-School & Infant Children			
I have read through the agreement and gone through it as appropriate with my child and agree to adhere to it. Please sign below on behalf of your child:			
Signed by Parent/Carer:		Date:	

Junior Children			
I have read and understand the School Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.			
Signed by Child:		Date:	

Parent's Consent for Internet Access			
I have read and understood the School rules for responsible Internet use and give permission for my child to access the Internet. I understand that the School will take all reasonable precautions to ensure children cannot access inappropriate materials. I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the School is not liable for any damages arising from use of the Internet facilities.			
Signed by Parent/Carer:		Date:	

Appendix 2 – Incident sheet from Online Safety Reporting Log.

Online Safety Reporting Log.

Read notes 'Responding to incident of misuse'.

Incident				Action taken		
Date	Time	Incident	Incident reported by:	By who?	What action was taken?	Signature