New Horizons Seaside Primary

Online Safeguarding and Acceptable Use of ICT Policy September 2024

Last Review Date:	Sept 2024
Next Review Date:	Sept 2025
Reviewed By:	Mr Lee Murley (Headteacher / Chief Executive Officer)

Contents

Introduction

At New Horizons Seaside Primary, the safety of our children is of the utmost importance. This includes keeping them safe when using electronic equipment and more specifically when entering the online world.

E-safety encompasses internet technologies and also electronic communications via mobile phones, games consoles and wireless technology. By educating our children in e-safety we aim to highlight the need for children and young people to think practically about the benefits, risks and responsibilities of using information technology.

To ensure all of our children are aware of the potential dangers, we ensure that pupils are systematically educated in matters of e-safety at an age appropriate level throughout their time at New Horizons Seaside Primary, as part of their Computing lessons and in other areas of the curriculum where appropriate.

We operate an open-door policy for reporting issues relating to e-safety. Parents and carers should ask to speak with the dedicated Online Safeguarding Officer, Mr Murley, or in his absence, Mrs N Irwin, Mr R Nicholas or Mrs A Cornish about any perceived problems.

Development of the Policy

This E-Safety and Acceptable Use of ICT Policy has been developed by:

- Headteacher / CEO (Online Safeguarding Officer / E-Safety Officer)
- Deputy Headteachers
- Computing Curriculum Team
- Governor attached to Computing (ICT)
- Year 6 School Councillors

This policy is linked to, and works alongside the school's Child Protection Policy and the Anti-Bullying Policy. It is reviewed annually in consultation with the Governor responsible for e-safety.

Scope of the Policy

This policy applies to all members of the New Horizons Seaside Primary (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and who are users of ICT at New Horizons Seaside Primary.

New Horizons Seaside Primary will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within New Horizons Seaside Primary:

Online Safeguarding Governor

Governors are responsible for the approval of the Online Safeguarding Policy.

A named member of the Governing Body will be allocated the role of Online Safeguarding Governor and will be responsible for reviewing the effectiveness of the policy.

The role of the Online Safeguarding Governor will include:

- regular updates from the Online Safeguarding Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

Online Safeguarding Officer

Headteacher (CEO): Mr L Murley: Online Safeguarding Officer (ESO) / Child Protection Officer (CPO)
Senior Deputy Headteacher: Mrs N Irwin ESO / CPO
Deputy Head: Mr R Nicholas ESO / CPO
Assistant Headteacher for Inclusion: Mrs A Cornish ESO / CPO

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community. In this capacity, the Headteacher acts as the Online Safeguarding Officer, part of the role of Child Protection Officer.

Any e-safety issues or incidents concerning children which arise in class or which come to the attention of staff or parents / carers of children at New Horizons Seaside Primary should be passed on to the Headteacher as a matter of urgency.

In the absence of the Headteacher, another ESO / CPO as named above will assume this role.

All ESOs / CPOs should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. See the flow chart on dealing with e-safety incidents – “Responding to incidents of misuse” – on pages 4 – 5 and the protocol for dealing with other incidents on pages 5 – 6.

Responsibilities:

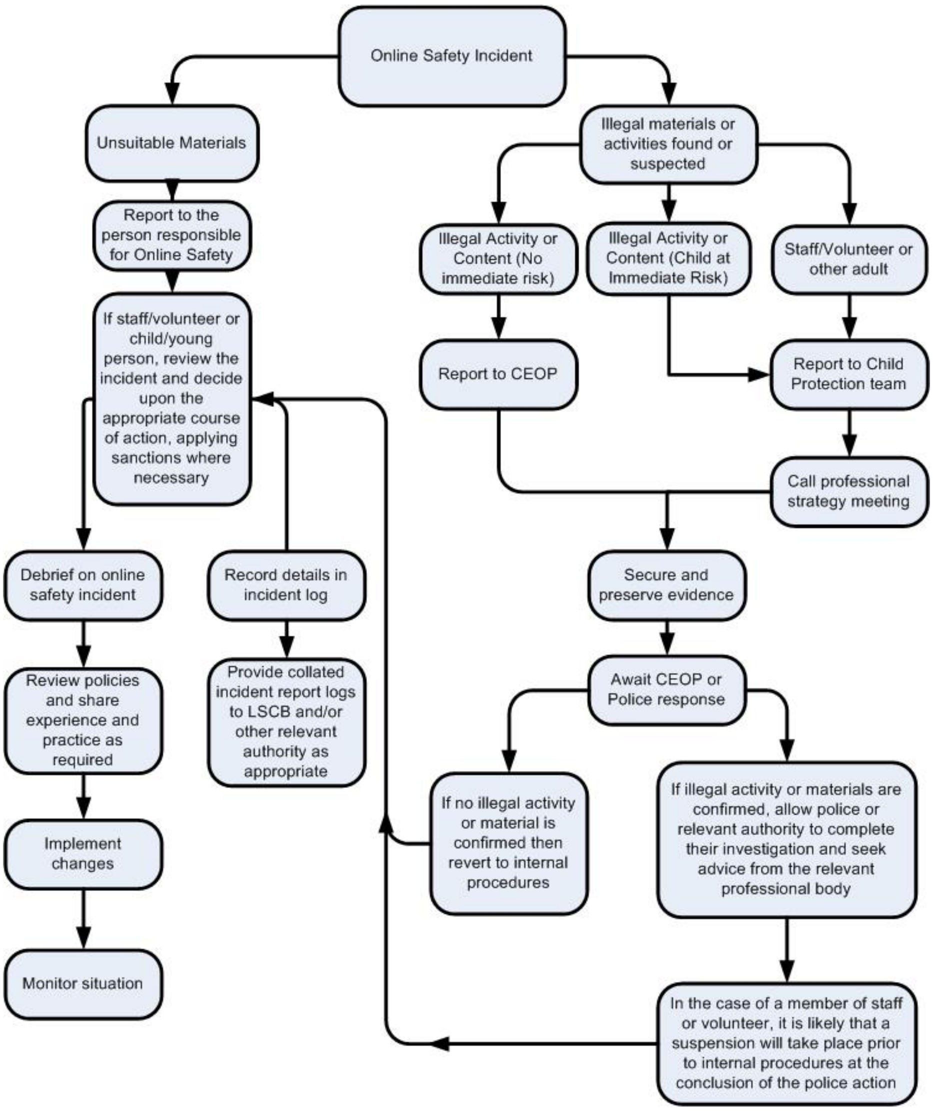
- To take day to day responsibility for any e-safety issues which arise.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- To provide training and advice for staff
- To monitor that office staff are updating Class Consent Form overviews and that these are available on the school system.
- To liaise with school technical staff
- To receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments,
- To meet regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- To attend relevant Governor meetings
- To attend training in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - ➢ sharing of personal data
    - ➢ access to illegal / inappropriate materials
    - ➢ inappropriate on-line contact with adults / strangers
    - ➢ potential or actual incidents of grooming
    - ➢ cyber-bullying

Protocol for responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police.


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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
    - **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the New Horizons Seaside Primary and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained for evidence and reference purposes.

Online Safeguarding Coordinator

The role of Online Safeguarding Coordinator is carried out by a named member of staff, working in conjunction with those teachers who form the Computing Curriculum Team.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Responsibilities:

- To ensure that pupils are systematically educated in matters of e-safety at an age appropriate level throughout their time at New Horizons Seaside Primary.
- To update annually an E-Safety Long Term Plan for all year groups showing where e-safety is to be taught in Computing across New Horizons Seaside Primary and to monitor through planning and work checks that this plan is being implemented (see Appendix C on page 16).
- To ensure that e-safety issues are addressed in other areas of the curriculum and other activities where appropriate i.e. 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.
- To oversee the active implementation and reinforcement of the Pupil Acceptable Use Policy by teachers at New Horizons Seaside Primary, regarding pupils' use of ICT in and out of school.
- To monitor that pupils understand and follow the Pupil Acceptable Use Policy.
- To ensure that key e-Safety messages should be reinforced as part of a planned programme of assemblies at an age appropriate level.

IT Technician: JSPC

Our broadband is provided through OpenHive and all web filtering meets government and BECTA standards. All internet access provided to staff and children is filtered through OpenHive Webshield, which automatically prohibits access to inappropriate sites. All staff and children are aware of the filtering system.

Responsibilities:

- To ensure that New Horizons Seaside Primary's technical infrastructure is secure and is not open to misuse or malicious attack
- To ensure that New Horizons Seaside Primary meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher
- that monitoring software / systems are implemented and updated as agreed in school policies Technical – infrastructure / equipment, filtering and monitoring

- The Seaside ICT technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is regularly monitored
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school: See School Laptop Loan Agreement / School Tablet Loan Agreement (Appendix D on page 17 and Appendix E on page 20).
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Children are not allowed to use mobile phones on the premises at New Horizons Seaside Primary. If parents / carers of KS2 children wish their child to bring a phone into school, it is the child's responsibility to ensure that the phone is handed to the school office for safekeeping at the start of the day and to remember to collect the phone at the end of the day.

A phone which is not handed in will be confiscated until the parent / carer can come into school to personally collect the phone from the office. Children are not allowed to take mobile phones on school trips or on residential visits.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)
- Supporting New Horizons Seaside Primary in the event of sanctions as outlined in the Pupil Acceptable Use policy being applied to their child following a thorough investigation of a given incident or issue.

Teachers / Seaside Staff: See the Staff Acceptable Use of ICT Policy (Appendix A on page 9).

Pupils: See the Pupil Acceptable Use of ICT Policy (Appendix B on page 14).

Appendix A

New Horizons Seaside Primary
Staff Acceptable Use of ICT Policy

For all staff working at New Horizons Seaside Primary including Senior Leaders, Teachers, Teaching Assistants and Office Staff

School networked resources, including SIMS and SIMS Learning Gateway, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school, County Council or Trust then you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school, County Council or Trust into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Please read the following document carefully if you are a member of staff at New Horizons Seaside Primary. Once you have read through the document, please ensure you ask questions about any points you are unsure of. Once satisfied, please sign the declaration and hand this in to the E-Safety Officer (Lee Murley).

General Responsibilities:

1. I will ensure I have an up to date awareness of e-safety matters and of the current school New Horizons Seaside Primary E-Safety Policy and practices (saved to T-Drive – Teacher Folders – Policies / on school website in Statutory Information – Policies).
2. I will raise any concerns regarding e-safety (relating to pupils or staff) in confidence at the earliest opportunity to the Headteacher and in his absence the Senior Deputy Headteacher, the Deputy Head or the Assistant Headteacher for Inclusion for investigation / action / sanction.
3. I will read, sign and follow this Staff Acceptable Use Policy (AUP).
4. I will sign and adhere to the New Horizons Seaside Primary School Laptop Loan Agreement.
5. I will sign and adhere to the New Horizons Seaside Primary School Tablet Loan Agreement.
6. I will sign and adhere to the New Horizons Seaside Primary School SIMS MIS Acceptable Use Policy.
7. I will ensure that all digital communications I undertake with parents / carers are on a professional level and only carried out using official school systems.

Classroom Responsibilities:

1. I will ensure that e-safety issues are addressed in my year group by following the E-Safety Long Term Plan and I will ensure e-safety issues are addressed in other areas of the curriculum and other activities where appropriate.
2. I will ensure I play my part in ensuring my pupils participate in nationwide initiatives such as Safer Internet Day.
3. I will ensure KS1 pupils understand and follow the Pupil Acceptable Use Policy at an age-appropriate level through verbal reminders and input in lessons.
4. I will ensure KS2 pupils read and understand the Pupil Acceptable Use Policy; I will ensure KS2 pupils understand the need for the Pupil Acceptable Use Policy; I will ensure that my class sign the Pupil Acceptable Use Policy at the start of each year and follow the policy throughout the year.
5. I will ensure that pupils understand the need to avoid plagiarism and uphold copyright regulations when using the internet for research.

6. I will monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed).
7. I will ensure that parental / carer permission has been granted for individual pupils to use the internet in school (refer to the Class Consent Form overview on the T-Drive).
8. I will ensure that in lessons where internet use is pre-planned, pupils are 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.
9. In lessons where pupils are allowed to freely search the internet, I will be vigilant in monitoring the content of the websites the pupils visit.
10. I will ensure that any work published on the school website or on Google APPs for Education is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff.
11. I will only use un-named images of groups of pupils in newsletters, on the website etc as outlined on the Parent / Carer consent form with parental / carer consent.
12. I will ensure any images of pupils are appropriately stored and secured on the school's network.
13. I will always aim to use a school camera in the first instance, but if I do need to use my own camera or mobile phone to record images, I will ensure these images are downloaded onto the school network at the earliest opportunity for storage and nowhere else and I will delete these images from my phone or camera as soon as possible.
14. I will not communicate with children via personal email or mobile phone. The only exception to this is email correspondence using the Google email (Seaside address) for discussion of work the children have submitted. This correspondence is logged and monitored.
15. I will not release or in any way make available my own personal details or the personal details of any colleague or pupil (phone numbers or personal e-mail addresses) over the Internet.
16. I may only download music at school if this is done legally and in line with copyright laws.
17. I will ensure that I will maintain files and folders I have saved on the network server and keep the size of these files and folders to a level suitable for our available storage capacity.
18. I will ensure that children understand they are NOT allowed to use interactive whiteboards or to have free access to the Internet at lunchtime if it is wet break.

User personal and system security code of conduct / Personal Data regarding Pupils or Staff:

1. I must protect my own login details as a matter of personal and system security. I should not allow **any other users** to have my details or use my login.
2. If at any time I feel that my password has been seen by another user, I should logon and change my password immediately.
3. I must ensure that any device (tablet, laptop, memory stick or any other removable media) which I use to store personal data about pupils or staff is password protected, understanding that my equipment is more vulnerable once it leaves the building.
4. I will ensure that the above devices are properly "logged-off" at the end of any session in which they are used to access personal data. If accessing school data from home on personal or school provided hardware, I will always ensure, by following the aforementioned code, that data integrity is respected at all times.
5. I will ensure that visitors to the school, including supply teachers, student teachers or parent helpers, do not have access to the school T-Drive, which contains confidential information about pupils as well as being used to store Seaside planning and proformas.
   Folders on the N-Drive should be created by the host teacher for use by the supply teachers or student teachers. These folders can be used to contain teaching resources (Smart Notebooks or Powerpoint Presentations etc) as well as planning with pupil names removed. Any access of the T-Drive by supply teachers or student teachers should be in the presence of and supervised at all times by the host teacher.

6. If I find an unattended machine logged on under any other user's username, I will **not** continue using the machine – I will log it off immediately.
7. I will not trespass into other users' files or folders.
8. I will not use the network in any way that would disrupt use of the network by others.
9. I will not use personal "USB drives", portable hard-drives, tablets or personal laptops on the network without having them "approved" by the IT Technician (JSPC) and checked for viruses. Student teachers should also ensure that their devices have been checked by the IT Technician – see also Point 3 of this section.
10. I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed. If in doubt, I will check with the IT Technician. '
11. I will not use remote access on a public computer.
12. I will not use remote desktop on a personal computer that is used by other members of the household.
13. I will not save my password on the remote access icon.

Responsibilities regarding Online Publishing and Social Media – Protecting Professional Identity:

1. I will not create, transmit, display or publish any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person or bring the school, Trust or West Sussex County Council into disrepute.
2. I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. I will not refer in social media to pupils, parents / carers or school staff.
5. I will not engage in online discussion on personal matters relating to members of the school community.
6. I will not attribute any personal opinions to New Horizons Seaside Primary.
7. I will regularly check the security settings on any personal social media profiles I use to minimize the risk of loss of personal information.
8. I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.
9. I will not accept invitations from parents of pupils in New Horizons Seaside Primary to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.
10. As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends.

Unsuitable / inappropriate activities

New Horizons Seaside Primary believes that the activities referred to in this table would be inappropriate in a school context and that all staff should not engage in these activities in school **or outside school when using school equipment or systems**. The school policy restricts usage as follows: **User Actions**		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce – unless buying resources for school.					X	
File sharing (e.g. sharing between school GAFE accounts)				X		
Use of social media					X	
Use of messaging apps					X	
Use of video broadcasting eg. Youtube				X		

New Horizons Seaside Primary Staff Acceptable Use Policy

Staff User Agreement Form

For all staff working at New Horizons Seaside Primary including Senior Leaders, Teachers, Teaching Assistants and Office Staff.

I confirm that I have read the latest version of the New Horizons Seaside Primary E-Safety and Acceptable Use of ICT Policy and I understand my responsibilities as a member of staff at New Horizons Seaside Primary as outlined in the aforementioned policy on pages 9 – 12 as well as my responsibilities regarding the use of the Arbor MIS on pages 24 – 25.

I have taken the opportunity to ask the E-Safety Officer (Mr L Murley) any questions I might have. I confirm that these points have been satisfactorily clarified.

If I am in any doubt, I will consult a member of SLT or the IT Technician (JSPC).

I agree to report any misuse of the network or any other concerns to the Headteacher or in his absence, the Senior Deputy Headteacher, the Deputy Head or the Assistant Headteacher for Inclusion.

I agree to report any websites that are available on the school Internet that contain inappropriate material to the Headteacher and also to the IT Technician.

If I do not follow the rules and responsibilities as outlined in the New Horizons Seaside Primary E-Safety and Acceptable Use of ICT Policy, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Signed: ______________________________

Name: ______________________________

Position at New Horizons Seaside Primary: ______________________________

Date: ____________________

New Horizons Seaside Primary
KS2 Pupil Acceptable Use of ICT Policy

Appendix B

Name: ___________________________

I understand I must follow the rules in this policy when using school computers.

If I do not follow these rules I may find:

- **I am not allowed to use the computers.**
- **I can only use the computers when supervised.**
- **I may have my GAFE (Google Apps for Education) account blocked for a while**.

My teachers will show me how to use the computers.

UNACCEPTABLE USE – What I am NOT allowed to do!

- I must NOT use a computer with another person's username and password.
- I must NOT create or send on the Internet any messages that might upset other people.
- I must NOT look at, or change work that belongs to other people.
- I must NOT waste time or resources on school computers.
- I must NOT try to look at inappropriate material / click on any pop-ups that may appear.

What to do if you see something that concerns you

It is likely that at some point you will come across some images or words that you did not intend to see. If this happens and you do see or hear something that scares, worries or upsets you do the following immediately:

- Turn the computer screen off! Do not turn the PC off.
- Put your hand up and ask for a teacher to come straight over.
- DO NOT show other students what you have seen or discuss this with them.
- Wait for someone to come over and help you quietly.

Your teacher will then tell you what to do next.

Code of conduct for children – Read this carefully!

Look after yourself! Never give any information which would help anyone work out where you live or who you are. You would not give your name and address to a stranger you meet at a bus stop, so do not give your full name, telephone number or address when working on the Internet. The same applies about giving information about your family and friends.

Never arrange to meet people over the internet. Remember, not everyone you 'meet' on-line are who they say they are. People can pretend to be someone else.

Any password you create is secret. Only share it with parents/carers. If you think someone else has found out your password, tell your teacher straight away.

Never delete, change or read other people's e-mails, files or passwords. We share our network so remember to be careful. You do not want your work deleted or changed, so don't do it to others. Never attempt to log on as somebody else, and never leave a computer logged on to your own username.

Be polite to others when online, just as you should be in school. The same rules for the classroom and playground apply online, so swearing, rudeness and threatening language are not allowed. Never write anything online which would give the school a bad name.

Look after the school's equipment. Treat the school's computers with care. Leave laptops and tablets charging once you have finished using them.

Only use the interactive whiteboards, school cameras and other equipment if you have been given permission by an adult.

Only use appropriate material. If you come across things that are deliberately rude, disrespectful, illegal or things that make you feel uncomfortable, tell an adult, who will inform our E-Safety Officer. If you receive messages that would break these rules, tell an adult immediately.

Never deliberately look for things you know are not allowed. Your teacher can and will check what you have been doing on the school's computers.

Just because it comes out of a computer, that does not mean it is true! Some people make up things. Always check where the information has come from and check it.

If music is free to download, then it may be illegal. Don't listen to music or watch videos in school that are rude, racist or meant for older children or adults.

Remember: the whole world is watching!

I agree to follow the school rules when using the school computers. I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the computers sensibly to my teacher.

I also agree to tell my teacher if I see any websites that make me feel unhappy or uncomfortable.
If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Pupil Name: ______________________________ Y3 Class:_____________________ Date: _______________

Pupil Name: ______________________________ Y4 Class:_____________________ Date: _______________

Pupil Name: ______________________________ Y5 Class:_____________________ Date: _______________

Pupil Name: ______________________________ Y6 Class:_____________________ Date: _______________

Parent / Carer to complete below at Autumn Parents Evening when their child is in Year 3 (or at the earliest opportunity if their child joins New Horizons Seaside Primary later than this).

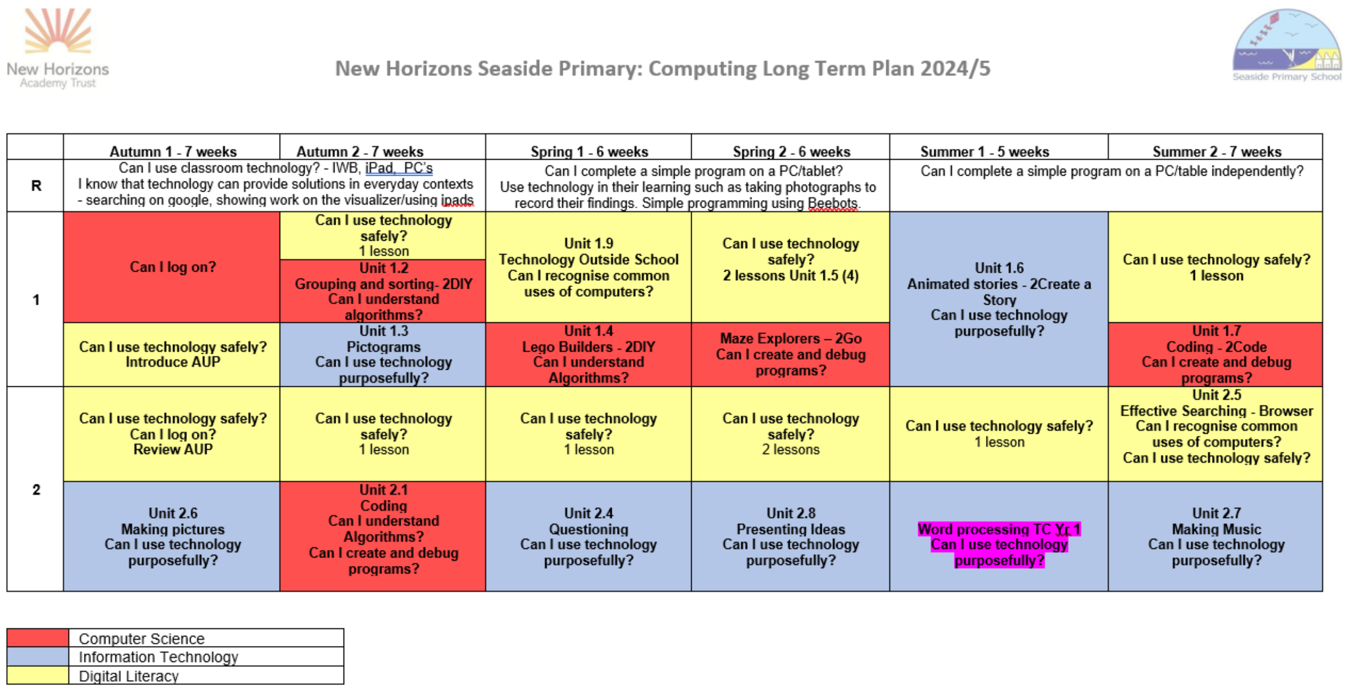
I realise that any pupil under reasonable suspicion of not following the rules, shown above in the policy, when using (or misusing) the computers may have their use stopped, more closely monitored or past use investigated.

Parent/Carers Name: _________________________ Parent/Carers Signature: ______________________

Date: ________________

Appendix C

New Horizons Seaside Primary
Long Term Computing Plan with
NHSP Online Safeguarding (OS) Long Term Plan
(See 'Curriculum' Section in Statutory Information on website)



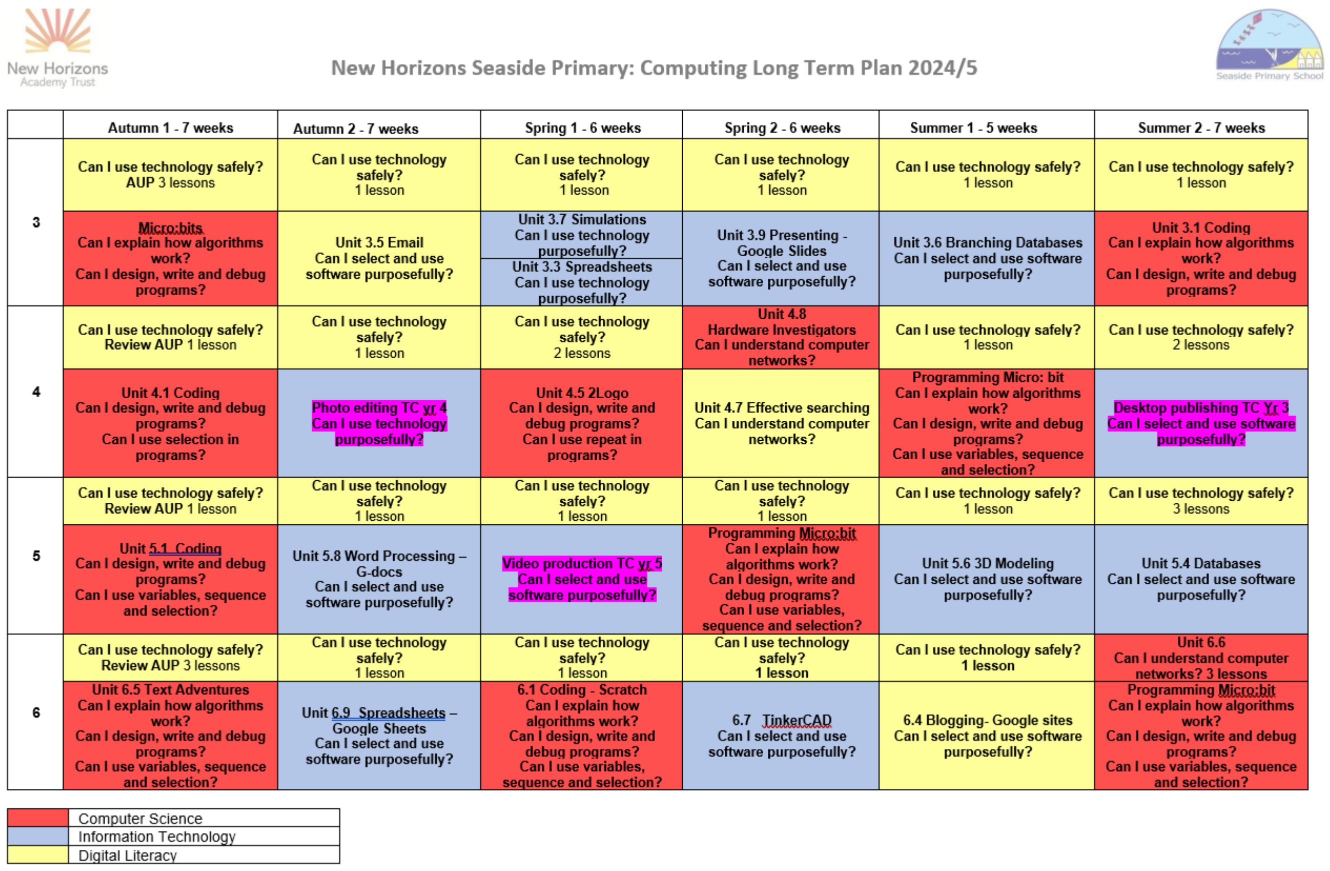
New Horizons Academy Trust

New Horizons Seaside Primary: Computing Long Term Plan 2024/5

Seaside Primary School

	Autumn 1 - 7 weeks	Autumn 2 - 7 weeks	Spring 1 - 6 weeks	Spring 2 - 6 weeks	Summer 1 - 5 weeks	Summer 2 - 7 weeks
R	Can I use classroom technology? - IWB, iPad, PC's I know that technology can provide solutions in everyday contexts - searching on google, showing work on the visualizer/using ipads		Can I complete a simple program on a PC/tablet? Use technology in their learning such as taking photographs to record their findings. Simple programming using Beebots.		Can I complete a simple program on a PC/table independently?	
1	Can I log on?	Can I use technology safely? 1 lesson Unit 1.2 Grouping and sorting- 2DIY Can I understand algorithms?	Unit 1.9 Technology Outside School Can I recognise common uses of computers?	Can I use technology safely? 2 lessons Unit 1.5 (4)	Unit 1.6 Animated stories - 2Create a Story Can I use technology purposefully?	Can I use technology safely? 1 lesson
	Can I use technology safely? Introduce AUP	Unit 1.3 Pictograms Can I use technology purposefully?	Unit 1.4 Lego Builders - 2DIY Can I understand Algorithms?	Maze Explorers – 2Go Can I create and debug programs?		Unit 1.7 Coding - 2Code Can I create and debug programs?
2	Can I use technology safely? Can I log on? Review AUP	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 2 lessons	Can I use technology safely? 1 lesson	Unit 2.5 Effective Searching - Browser Can I recognise common uses of computers? Can I use technology safely?
	Unit 2.6 Making pictures Can I use technology purposefully?	Unit 2.1 Coding Can I understand Algorithms? Can I create and debug programs?	Unit 2.4 Questioning Can I use technology purposefully?	Unit 2.8 Presenting Ideas Can I use technology purposefully?	Word processing TC Yr 1 Can I use technology purposefully?	Unit 2.7 Making Music Can I use technology purposefully?

🟥	Computer Science
🟦	Information Technology
🟨	Digital Literacy



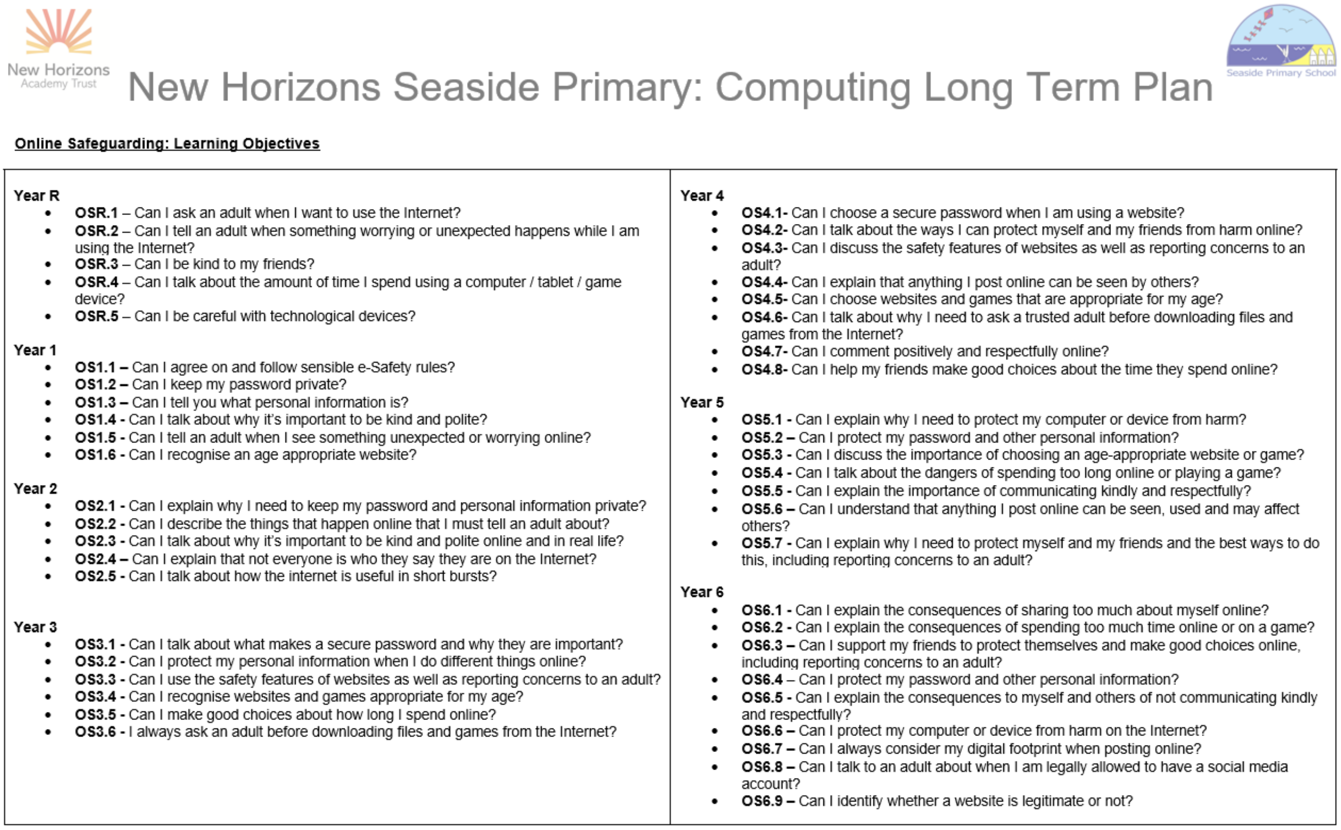
New Horizons Academy Trust

New Horizons Seaside Primary: Computing Long Term Plan 2024/5

Seaside Primary School

	Autumn 1 - 7 weeks	Autumn 2 - 7 weeks	Spring 1 - 6 weeks	Spring 2 - 6 weeks	Summer 1 - 5 weeks	Summer 2 - 7 weeks
3	Can I use technology safely? AUP 3 lessons	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson
	Micro:bits Can I explain how algorithms work? Can I design, write and debug programs?	Unit 3.5 Email Can I select and use software purposefully?	Unit 3.7 Simulations Can I use technology purposefully? Unit 3.3 Spreadsheets Can I use technology purposefully?	Unit 3.9 Presenting - Google Slides Can I select and use software purposefully?	Unit 3.6 Branching Databases Can I select and use software purposefully?	Unit 3.1 Coding Can I explain how algorithms work? Can I design, write and debug programs?
4	Can I use technology safely? Review AUP 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 2 lessons	Unit 4.8 Hardware Investigators Can I understand computer networks?	Can I use technology safely? 1 lesson	Can I use technology safely? 2 lessons
	Unit 4.1 Coding Can I design, write and debug programs? Can I use selection in programs?	Photo editing TC yr 4 Can I use technology purposefully?	Unit 4.5 2Logo Can I design, write and debug programs? Can I use repeat in programs?	Unit 4.7 Effective searching Can I understand computer networks?	Programming Micro: bit Can I explain how algorithms work? Can I design, write and debug programs? Can I use variables, sequence and selection?	Desktop publishing TC Yr 3 Can I select and use software purposefully?
5	Can I use technology safely? Review AUP 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 3 lessons
	Unit 5.1 Coding Can I design, write and debug programs? Can I use variables, sequence and selection?	Unit 5.8 Word Processing – G-docs Can I select and use software purposefully?	Video production TC yr 5 Can I select and use software purposefully?	Programming Micro:bit Can I explain how algorithms work? Can I design, write and debug programs? Can I use variables, sequence and selection?	Unit 5.6 3D Modeling Can I select and use software purposefully?	Unit 5.4 Databases Can I select and use software purposefully?
6	Can I use technology safely? Review AUP 3 lessons	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Can I use technology safely? 1 lesson	Unit 6.6 Can I understand computer networks? 3 lessons
	Unit 6.5 Text Adventures Can I explain how algorithms work? Can I design, write and debug programs? Can I use variables, sequence and selection?	Unit 6.9 Spreadsheets – Google Sheets Can I select and use software purposefully?	6.1 Coding - Scratch Can I explain how algorithms work? Can I design, write and debug programs? Can I use variables, sequence and selection?	6.7 TinkerCAD Can I select and use software purposefully?	6.4 Blogging- Google sites Can I select and use software purposefully?	Programming Micro:bit Can I explain how algorithms work? Can I design, write and debug programs? Can I use variables, sequence and selection?

🟥	Computer Science
🟦	Information Technology
🟨	Digital Literacy



New Horizons Seaside Primary: Computing Long Term Plan

Online Safeguarding: Learning Objectives

Year R

- **OSR.1** – Can I ask an adult when I want to use the Internet?
- **OSR.2** – Can I tell an adult when something worrying or unexpected happens while I am using the Internet?
- **OSR.3** – Can I be kind to my friends?
- **OSR.4** – Can I talk about the amount of time I spend using a computer / tablet / game device?
- **OSR.5** – Can I be careful with technological devices?

Year 1

- **OS1.1 –** Can I agree on and follow sensible e-Safety rules?
- **OS1.2 –** Can I keep my password private?
- **OS1.3 –** Can I tell you what personal information is?
- **OS1.4 -** Can I talk about why it's important to be kind and polite?
- **OS1.5 -** Can I tell an adult when I see something unexpected or worrying online?
- **OS1.6 -** Can I recognise an age appropriate website?

Year 2

- **OS2.1 -** Can I explain why I need to keep my password and personal information private?
- **OS2.2 -** Can I describe the things that happen online that I must tell an adult about?
- **OS2.3 -** Can I talk about why it's important to be kind and polite online and in real life?
- **OS2.4 –** Can I explain that not everyone is who they say they are on the Internet?
- **OS2.5 -** Can I talk about how the internet is useful in short bursts?

Year 3

- **OS3.1 -** Can I talk about what makes a secure password and why they are important?
- **OS3.2 -** Can I protect my personal information when I do different things online?
- **OS3.3 -** Can I use the safety features of websites as well as reporting concerns to an adult?
- **OS3.4 -** Can I recognise websites and games appropriate for my age?
- **OS3.5 -** Can I make good choices about how long I spend online?
- **OS3.6 -** I always ask an adult before downloading files and games from the Internet?

Year 4

- **OS4.1-** Can I choose a secure password when I am using a website?
- **OS4.2-** Can I talk about the ways I can protect myself and my friends from harm online?
- **OS4.3-** Can I discuss the safety features of websites as well as reporting concerns to an adult?
- **OS4.4-** Can I explain that anything I post online can be seen by others?
- **OS4.5-** Can I choose websites and games that are appropriate for my age?
- **OS4.6-** Can I talk about why I need to ask a trusted adult before downloading files and games from the Internet?
- **OS4.7-** Can I comment positively and respectfully online?
- **OS4.8-** Can I help my friends make good choices about the time they spend online?

Year 5

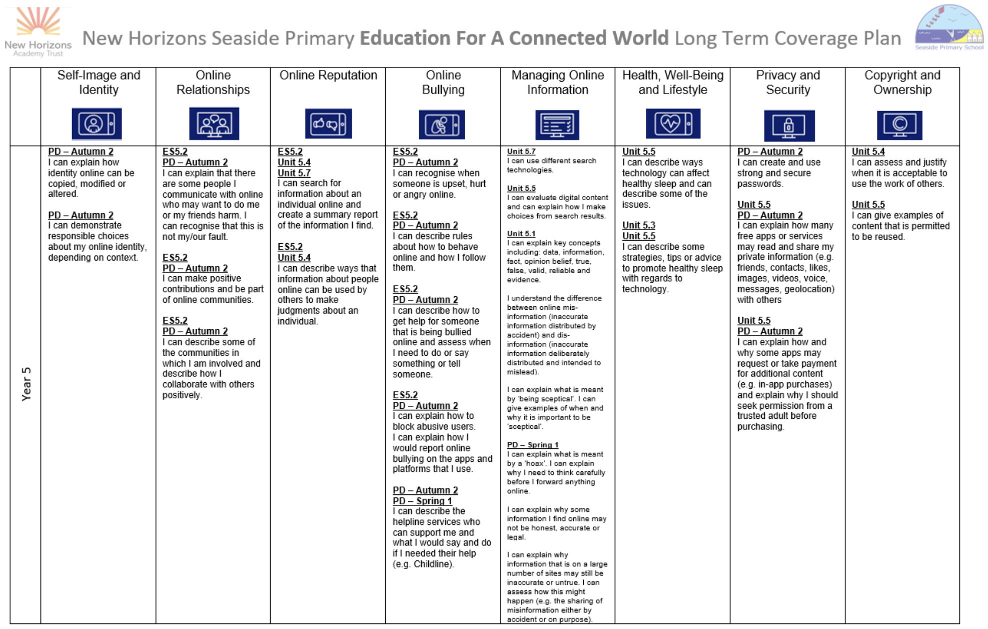
- **OS5.1 -** Can I explain why I need to protect my computer or device from harm?
- **OS5.2 –** Can I protect my password and other personal information?
- **OS5.3 -** Can I discuss the importance of choosing an age-appropriate website or game?
- **OS5.4 -** Can I talk about the dangers of spending too long online or playing a game?
- **OS5.5 -** Can I explain the importance of communicating kindly and respectfully?
- **OS5.6 –** Can I understand that anything I post online can be seen, used and may affect others?
- **OS5.7 -** Can I explain why I need to protect myself and my friends and the best ways to do this, including reporting concerns to an adult?

Year 6

- **OS6.1 -** Can I explain the consequences of sharing too much about myself online?
- **OS6.2 -** Can I explain the consequences of spending too much time online or on a game?
- **OS6.3 –** Can I support my friends to protect themselves and make good choices online, including reporting concerns to an adult?
- **OS6.4** – Can I protect my password and other personal information?
- **OS6.5 -** Can I explain the consequences to myself and others of not communicating kindly and respectfully?
- **OS6.6 –** Can I protect my computer or device from harm on the Internet?
- **OS6.7 –** Can I always consider my digital footprint when posting online?
- **OS6.8 –** Can I talk to an adult about when I am legally allowed to have a social media account?
- **OS6.9 –** Can I identify whether a website is legitimate or not?

In addition to the NHSP Online Safeguarding Long Term Plan, please also refer to the New Horizons Seaside Primary **Education For A Connected World** Long Term Coverage Plan (on the school website) which states when the Education For A Connected World framework objectives are delivered to pupils across their time at New Horizons Seaside Primary. Where there is a crossover with the NHSP Online Safeguarding objectives, this is noted on the plan.

https://www.thinkuknow.co.uk/professionals/guidance/ukccis-framework-education-for-a-connected-world/



New Horizons Seaside Primary **Education For A Connected World** Long Term Coverage Plan

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Managing Online Information	Health, Well-Being and Lifestyle	Privacy and Security	Copyright and Ownership
Year 5	PD – Autumn 2 I can explain how identity online can be copied, modified or altered. PD – Autumn 2 I can demonstrate responsible choices about my online identity, depending on context.	ES5.2 PD – Autumn 2 I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault. ES5.2 PD – Autumn 2 I can make positive contributions and be part of online communities. ES5.2 PD – Autumn 2 I can describe some of the communities in which I am involved and describe how I collaborate with others positively.	ES5.2 Unit 5.4 Unit 5.7 I can search for information about an individual online and create a summary report of the information I find. ES5.2 Unit 5.4 I can describe ways that information about people online can be used by others to make judgments about an individual.	ES5.2 PD – Autumn 2 I can recognise when someone is upset, hurt or angry online. ES5.2 PD – Autumn 2 I can describe rules about how to behave online and how I follow them. ES5.2 PD – Autumn 2 I can describe how to get help for someone that is being bullied online and assess when I need to do or say something or tell someone. ES5.2 PD – Autumn 2 I can explain how to block abusive users. I can explain how I would report online bullying on the apps and platforms that I use. PD – Autumn 2 PD – Spring 1 I can describe the helpline services who can support me and what I would say and do if I needed their help (e.g. Childline).	Unit 5.7 I can use different search technologies. Unit 5.5 I can evaluate digital content and can explain how I make choices from search results. Unit 5.1 I can explain key concepts including: data, information, fact, opinion belief, true, false, valid, reliable and evidence. I understand the difference between online mis-information (inaccurate information distributed by accident) and dis-information (inaccurate information deliberately distributed and intended to mislead). I can explain what is meant by 'being sceptical'. I can give examples of when and why it is important to be 'sceptical'. PD – Spring 1 I can explain what is meant by a 'hoax'. I can explain why I need to think carefully before I forward anything online. I can explain why some information I find online may not be honest, accurate or legal. I can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen (e.g. the sharing of misinformation either by accident or on purpose).	Unit 5.5 I can describe ways technology can affect healthy sleep and can describe some of the issues. Unit 5.3 Unit 5.5 I can describe some strategies, tips or advice to promote healthy sleep with regards to technology.	PD – Autumn 2 I can create and use strong and secure passwords. Unit 5.5 PD – Autumn 2 I can explain how many free apps or services may read and share my private information (e.g. friends, contacts, likes, images, videos, voice, messages, geolocation) with others Unit 5.5 PD – Autumn 2 I can explain how and why some apps may request or take payment for additional content (e.g. in-app purchases) and explain why I should seek permission from a trusted adult before purchasing.	Unit 5.4 I can assess and justify when it is acceptable to use the work of others. Unit 5.5 I can give examples of content that is permitted to be reused.

New Horizons Seaside Primary
School Laptop Loan Agreement

Appendix D

New Horizons Seaside Primary provides laptop computers to teachers to assist in the delivery of the Curriculum. The Headteacher has agreed that a laptop computer will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time.

As a member of staff to whom a laptop has been loaned I have read and agree to the following terms and conditions that apply while the laptop is in my possession:

1	The Laptop - and any accessories provided with it - remains the property of *New Horizons Seaside Primary* and is strictly for my sole use in assisting in the delivery of the Curriculum.
2	I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the laptop is stolen from an unattended vehicle or a house left unattended for longer than 48 hours, I will be responsible for its replacement.
3	I agree to: treat the laptop with due care and keep the laptop in good condition, ensure that it is strapped in to the carry case when transported and/or not in use, not leave the laptop unattended in class without being secured and avoid food and drink near the keyboard/touch pad.
4	I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the laptop malfunctioning.
5	I agree to only use software licensed by the school, authorised by the Headteacher and installed by the school's ICT staff.
6	I agree that Anti-Virus software is installed and must be updated on a regular basis. ICT staff from the school will advise on the routines and schedule of this operation.
7	Should any faults occur, I agree to notify the school's ICT staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or any one other than ICT staff, attempt to fix suspected hardware, or any other faults.
8	I agree to attend training in how to access the Curriculum Network, Intranet, Internet, and email within the school provided by ICT staff.
9	I agree that home Internet access is permitted at the discretion of the Headteacher **for use relating to school work and appropriate personal use. Use outside of school by unauthorised personnel is not permitted.** I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.
10	I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.
11	I agree to adhere to School and LA policies regarding the following, updated as necessary:

	● Acceptable use ● Data protection ● Computer misuse ● Health and safety

Note on Insurance

For laptops to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the laptops for theft (where there are signs of forced entry), and accidental or malicious damage. Those Schools who have opted for the additional Buildings and Contents policy will also receive cover for flood/water damage, storm damage etc. All equipment in Schools is automatically covered for fire, lightning and explosion.

Laptops are not covered by the school policy:

- Whilst in vehicles
- Left unattended in a locked household over 48 hours.

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to ICT staff. If stolen or damaged from an employee's home, County would first ask for a claim under the staff member’s household policy. Claims from the School policy will only be made if this were unsuccessful.

Please note that regardless of the policy a stolen laptop is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

***** PLEASE RETAIN THIS INFORMATION FOR FUTURE REFERENCE *****

***** PLEASE RETURN THE ACCEPTANCE FORM ATTACHED. *****

Staff User Acceptance Form for the School Laptop Loan Agreement

*** Please return to the ICT Technician ***

Laptop Details

Laptop Make: _______________________ Model: _____________________

Serial Number: _____________________ School Code: _________

Personnel Details

Loan Authorised by: ______________________________

Authorised signatory: __________________ Date: _ _ /_ _ /_ _ _ _

I have read and agree to be bound by the terms and conditions (as set out in the School Laptop Loan Agreement). □ (please tick to accept)

Name of Member of Staff: ________________________________
(Print name)

Received by: _____________________ Date: _ _ /_ _ /_ _ _ _
(Staff member signature)

New Horizons Seaside Primary

Appendix E

School Tablet Loan Agreement

New Horizons Seaside Primary provides tablet computers to teachers / teaching assistants to assist in the delivery of the Curriculum. The Headteacher has agreed that a tablet computer will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time.

As a member of staff to whom a tablet has been loaned I have read and agree to the following terms and conditions that apply while the tablet is in my possession:

1	The tablet - and any accessories provided with it - remains the property of *Seaside Primary School* and is strictly for my sole use in assisting in the delivery of the Curriculum.
2	I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the laptop is stolen from an unattended vehicle or a house left unattended for longer than 48 hours, I will be responsible for its replacement.
3	I agree to: treat the tablet with due care and keep it in good condition, ensure that it is retained in its protective case when transported and/or not in use, not leave the tablet unattended in class without being secured and avoid food and drink near it.
4	I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the laptop malfunctioning.
5	I agree to only use software licensed by the school, authorised by the Headteacher and installed by the school's ICT staff.
6	I agree that Anti-Virus software is installed and must be updated on a regular basis. ICT staff from the school will advise on the routines and schedule of this operation.
7	Should any faults occur, I agree to notify the school's ICT staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT staff, attempt to fix suspected hardware, or any other faults.
8	I agree to attend training in how to access the Curriculum Network, Intranet, SIMS, Internet, and email within the school provided by ICT staff.
9	I agree that home Internet access is permitted at the discretion of the head teacher **for use relating to school work and appropriate personal use. Use outside of school by unauthorised personnel is not permitted.** I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.
10	I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.
11	I agree to adhere to School and LA policies regarding the following, updated as necessary: ● Acceptable use ● Data protection ● Computer misuse ● Health and safety

Note on Insurance

For tablets to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the tablets for theft (where there are signs of forced entry), and accidental or malicious damage. Those Schools who have opted for the additional Buildings and Contents policy will also receive cover for flood/water damage, storm damage etc. All equipment in Schools is automatically covered for fire, lightning and explosion.

Tablets are not covered by the school policy:

- Whilst in vehicles
- Left unattended in a locked household over 48 hours.

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to ICT staff. If stolen or damaged from an employee's home, County would first ask for a claim under the staff member's household policy. Claims from the School policy will only be made if this were unsuccessful.

Please note that regardless of the policy a stolen tablet is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

***** PLEASE RETAIN THIS INFORMATION FOR FUTURE REFERENCE *****

***** PLEASE RETURN THE ACCEPTANCE FORM ATTACHED. *****

Staff User Acceptance Form
for the School Tablet Loan Agreement

*** Please return to the ICT Technician ***

Tablet Details

Tablet Make: _______________________ Model: _____________________

Serial Number: _____________________ School Code: _________

Personnel Details

Loan Authorised by: ______________________________

Authorised signatory: __________________ Date: _ _ /_ _ /_ _ _ _

I have read and agree to be bound by the terms and conditions (as set out in the School Tablet Loan Agreement). □ (Please tick to accept)

Name of Member of Staff: ________________________________
(Print name)

Received by: _____________________ Date: _ _ /_ _ /_ _ _ _
(Staff member signature)

New Horizons Seaside Primary

Accessing the Arbor MIS (Management Information System) Acceptable Use Policy

Appendix F

This policy applies to all those who access New Horizons Seaside Primary's Arbor (School Information Management System). This policy applies whenever and wherever information is accessed, whether the computer equipment used is owned by New Horizons Seaside Primary or not.

Access is granted strictly on condition that the individual formally agrees to the terms of this Policy by signing the Agreement return slip included with this policy.

Authorised Arbor Users

Only relevant members of staff who are required access to confidential information in relation to the school and/or its students are provided with access to the New Horizons Seaside Primary Arbor system. They only have access to the information they require in order to facilitate their professional/educational obligations.

The School, for audit purposes, will retain the signed Agreement return slip. You will retain the Policy for your records.

The school is required to arrange the removal of access of users who are no longer entitled access to Arbor, and to amend user access rights as appropriate.

Acceptable Use of Arbor – All Users

1	Users are responsible for their proper, professional use of the system.
2	Conditions of use are respected and any breach of the conditions of use may lead to withdrawal of a user's access. In some instances, such a breach could lead to criminal prosecution; in the case of staff it may be considered a disciplinary matter.
3	The system should not be used in any way that might bring the good name of the School into disrepute.
4	Staff are expected to use the functions of Arbor solely for the purposes of which they are intended.
5	All users accept personal responsibility for reporting any misuse of the system to a member of the School Leadership Team.
6	No user should access, create, transmit, display or publish any material, including images and data from the Arbor system, which is likely to cause offence, inconvenience or needless anxiety to others.
7	No user should create, transmit, display or publish any material, including images and data from the Arbor system that might be considered defamatory.
8	Staff should not make unauthorised attempts to access data and resources on the Arbor system by bypassing security or passwords protections.
9	No user should take any action designed or likely to cause corruption or destruction of other users' data, or violate the privacy of others.
10	Users should inform the Headteacher immediately if a security problem is identified. They should not demonstrate this problem to other users.
11	Users should inform the School's IT Technician (JSPC) immediately if they appear to have access to content that is not authorised. They should not demonstrate this problem to other users.

Information Security

This Policy is intended to minimize security risks. These risks might affect the integrity of New Horizons Seaside Primary data, the authorised Arbor user and the individuals to which the Arbor data pertains.

Information made available through the Arbor system is confidential and protected by law under the Data Protection Act 1998. In order to comply with this Act:

1	Users must not distribute or disclose any information obtained from the Arbor system to any person(s) without prior agreed permission from the Headteacher or so as to facilitate the professional execution of their duties as a member of staff at New Horizons Seaside Primary.
2	Users should not attempt to access the Arbor system in any environment where the security of the information contained in the Arbor system may be placed at risk such as an Internet café or public place.
3	Users must not transfer information from the Arbor system to any form of portable media such as pen/flash drives or SD/MMC cards or by electronic means such as e-mail without the express permission of the school. If information transfer is required it is advisable that permission is declared in writing, either in print or via electronic methods (email) so the legitimacy of the information transfer can be verified if necessary.
4	Passwords for Arbor user accounts should be complex and consist of at least eight characters including a combination of capital letters, lower case letters and numbers. Ideally, at least one symbol should be included as well.
5	Users must always keep their individual user name and password confidential. These usernames and passwords must never be disclosed to any third party, including other staff members. Never use anyone else’s username or password to access the Arbor system.
6	If you think someone has learned your password then contact the school’s IT Technician (JSPC) in the first instance or change it immediately if possible.
7	Users should ensure that if Arbor is left open on a device and the device is to be left unattended that the device access is locked (Windows button+L or via ctrl+alt+del on a windows device). Arbor should only be open on a device when it is in use and closed at all other times. If a device is identified to have been left in a vulnerable state then the device should immediately be locked to ensure continued data protection. All staff members are aware of this.

Denial of Access

Users are liable for any potential misuse of the system and/or breach of the Data Protection Act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

New Horizons Seaside Primary reserves the right to revoke or deny access to the Arbor system of any user under the following circumstances:

- If the validity of responsibility is questioned.
- Where a user or users are found to be in breach of the Accessing the Arbor Acceptable Use Policy.
- If any child protection concerns are raised or disputes occur, the school will suspend access for all parties concerned pending investigation.
- If a user is identified as a security risk.
- If a user no longer requires access to the Arbor system as part of their role.

Arbor Staff Agreement Return Slip

I confirm that I have read and understood the terms and conditions of the Arbor Acceptable Use Policy; have retained a copy of said policy and sign to accept these terms.

Signature of Staff member:

…………………………………………………………………………………………….

Name of Staff member (print):

…………………………………………………………………………………………….

Date: ………/………/………………

Please return this slip to JSPC (IT Technician) directly or via the School Main Office.