

# Online Safety Policy

## Spring Term 2021

### For Schools within our Collaboration:



At the schools within our collaboration, we are committed to ensuring equality of education and opportunity for all pupils, staff, parents and carers receiving services from the school, irrespective of race, gender, disability, faith or religion or socio-economic background. All staff are expected to uphold and promote the fundamental principles of British values, and as such, the schools within our collaboration are fully committed to safeguarding and promoting the welfare of all our pupils including protection against radicalisation. We therefore aim to develop a culture of inclusion and diversity in which all those connected to the school feel proud of their identity and able to participate fully in school life. Our core purpose, values and ethos is embodied in our mission that everyone takes:

**P= personal**

**R= responsibility**

**I = in**

**D= delivering**

**E= excellence**

Frequency of Review:                      Annually

Reviewed and Approved by:      The Combined Committee of the Governing Body

Date:                                              Spring 2021

Date of Next Review:                      Spring 2022

Reviewer: Emily Davies, Alan Hughes, Emma Severn, Sam Arnold

Signed: ----- (Chair of Governing Body)      Date: -----

## **Contents**

<b>1. Aims</b>	<b>3</b>
<b>2. Legislation and Guidance</b>	<b>3</b>
<b>3. Roles and responsibilities</b>	<b>3</b>
<b>4. Educating pupils about online safety</b>	<b>6</b>
<b>5. Educating parents about online safety</b>	<b>6</b>
<b>6. Cyber-bullying</b>	<b>7</b>
<b>7. Acceptable use of the internet in school</b>	<b>7</b>
<b>8. Using devices outside school</b>	
<b>Staff using work devices outside school</b>	<b>8</b>
<b>Pupils loaning device to use outside school</b>	
<b>9. How the school will respond to issues of misuse</b>	<b>8</b>
<b>10. Training</b>	<b>8</b>
<b>11. GDPR</b>	<b>9</b>
<b>12. Monitoring Arrangements</b>	<b>9</b>
<b>13. Links with other policies</b>	<b>9</b>
<b>Appendix 1: EYFS and KS1 acceptable use agreement – internal (pupils and parents/carers)</b>	<b>10</b>
<b>Appendix 2: KS2 acceptable use agreement – internal (pupils and parents/carers)</b>	<b>11</b>
<b>Appendix 3: EYFS and KS1 acceptable use agreement - external (pupils and parents/carers)</b>	<b>12</b>
<b>Appendix 4: KS2 acceptable use agreement - external (pupils and parents/carers)</b>	<b>13</b>
<b>Appendix 5: Pupil Portable Device Loan Agreement for parents</b>	<b>14</b>
<b>Appendix 6: Pupil Portable Device Loan for children</b>	<b>16</b>

## 1. Aims

Sutton Road Primary and Nursery School and Holgate Primary School and Nursery is committed to innovative use of technologies to enhance the quality of teaching and learning. It is important for pupils to understand how to use technology responsibly to ensure their learning takes place safely.

This policy is supported by and reinforces the school's safeguarding procedures and has been agreed by the Senior Leadership Team and the Governing Body. All members of staff will be made aware of this policy as part of their induction. It will be reviewed and updated annually. Furthermore, it will be reviewed in response to changes in legislation/guidance or in the event of an online safety issue.

Our school aims to:

- › Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- › Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- › Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

## 2. Legislation and guidance

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

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- › [Relationships and sex education](#)
- › [Searching, screening and confiscation](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).


It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also draws upon the National Curriculum computing programmes of study.

## 2. Roles and responsibilities

<p><u>Governing Body</u></p>	<p>Governors are responsible for the approval of the policy and for reviewing the effectiveness of the policy.</p> <p>The members of the Governor body in the Life Skills take responsibility for Online Safety and their role is.</p> <ul style="list-style-type: none"><li>• To maintain an up to date awareness of any risks or threats of technology use, including changes to legislation affecting the governance of the policy.</li><li>• To maintain an awareness of the school's policy on online safety.</li><li>• To be kept up to date with training, identified risks and any incidents by the headteacher/ Online-Safety Coordinator</li></ul>
------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p><u>Executive Headteacher / Head of School</u></p>	<p>The Executive Headteacher/Head of School has overall responsibility for online-safety within the school as part of ensuring the safety of all pupils, staff and users of technology in school. Day-to-day responsibility of administering this policy is delegated to the Computing Lead</p> <p>The Executive Headteacher/Head of School will ensure that:</p> <ul style="list-style-type: none"> <li>• Regular online safety training is provided for staff and to the school community.</li> <li>• The online safety coordinator has access to appropriate CPD in order to undertake day-to-day duties.</li> <li>• All online safety incidents are dealt with promptly, appropriately and according to school policies.</li> </ul>
<p><u>Designated Safeguarding Leads</u></p>	<p>Details of the school's DSLs are set out in our safeguarding policy as well relevant job descriptions.</p> <p>The DSLs takes lead responsibility for online safety in school, in particular:</p> <ul style="list-style-type: none"> <li>• Supporting the Executive Headteacher/Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.</li> <li>• Working with the Executive Headteacher/Head of School and other staff, as necessary, to address any online safety issues or incidents.</li> <li>• Ensuring that any online safety incidents are logged (via CPOMS) and dealt with appropriately in line with this policy.</li> <li>• Ensuring that any incidents of cyber-bullying are logged (via CPOMS) and dealt with appropriately in line with the school anti-bullying policy.</li> <li>• Updating and delivering staff training on online safety.</li> <li>• Liaising with other agencies and/or external services if necessary.</li> <li>• Providing regular reports on online safety in school to the Executive Headteacher/Head of School and/or governing board.</li> </ul>
<p><u>Online Safety Coordinator / Computing lead</u></p>	<p>The Online Safety coordinator will:</p> <ul style="list-style-type: none"> <li>• Keep up to date with the latest risks to children whilst using technology.</li> <li>• To keep the website up to date in regards to support documents for parents and pupils.</li> </ul>
<p><u>Network Support</u></p>	<p>Network Support are responsible for:</p> <ul style="list-style-type: none"> <li>• Ensuring anti-virus software is up to date, fit for purposes and actively running on all machines.</li> <li>• Monitoring devices to ensure they are working correctly.</li> <li>• Providing network-wide online safety solutions including filtering.</li> <li>• Ensuring filtering levels are applied correctly to different users of technology in school.</li> <li>• Maintaining network passwords for all users and email passwords for staff</li> <li>• Network Support will be made aware of this policy before first working on the school infrastructure.</li> </ul>
<p><u>All Staff</u></p>	<p>Staff will be clear about the details of this policy. Any questions will be raised at the point of sharing. Staff will report any online safety incidents directly to the Executive Headteacher/Head of</p>

	<p>School for logging. The procedures outlined in this policy will then be followed by the relevant staff.</p> <p>Staff will provide curriculum online safety education to their class throughout every academic year and share the Acceptable Use Policy with pupils and ask them to sign this at the beginning of the school year agreeing to use computers safely. Online safety tips will be publicised on the school website.</p> <p>Staff will evaluate all websites/technologies and risk assess these before introducing them to the classroom. The school will send out regular updates to parents of any inappropriate content that is current in the news and community and place details of this on the school website/social media.</p> <p>School will ensure parents are signposted to online safety support through the school website.</p>
<p><u>All students</u></p>	<p>All pupils will be made aware of the Acceptable Use Policy and asked to sign this. They will receive education on online safety appropriate to their age as part of the school's computing curriculum. They will be clear about the steps they should take if they feel unsafe at any time whilst using school technologies. If pupils believe they have accessed something which may be unsafe, they will alert a member of staff.</p> <p>Pupils are taught about the use of CEOP button that is located on the school website, this allows pupils to report something they don't feel is appropriate.</p>  <p>DSLs are also updated where breaches of acceptable have occurred via monitoring software (SENSO or other equivalent software).</p>
<p><u>Visitors</u></p>	<p>It may be deemed appropriate for visitors to be given access to the school's internet connection for educational purposes during their visit. This decision is made by the Executive Headteacher/Head of School and the visitor(s) will be made aware of the acceptable use policy which they must sign. The procedures of the policy will apply if acceptable use is not made.</p>
<p><u>Parent/Carers/Community</u></p>	<p>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, local online safety campaigns, relevant websites and school social media.</p> <p>Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events. The school may provide training with technology or provide access to devices for parents/carers/the school community during the academic year. Users will be made aware of the acceptable use policy and asked to sign it. The procedures of the policy will apply if acceptable use is not made.</p>

## 4. Educating pupils about online safety

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

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

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

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

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact
- › By the end of primary school, pupils will know:
  - › That people sometimes behave differently online, including by pretending to be someone they are not.
  - › That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
  - › The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
  - › How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
  - › How information and data is shared and used online
  - › How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- › [KS2 Relationships education and health education](#)

The school will use additional activities (e.g. assemblies, external speakers and discrete sessions responding to specific issues raised) to raise pupils' awareness of the dangers that can be encountered online. Online safety is also covered in our Talking Point texts as part of our PSHCE curriculum.

## 5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher, who will then liaise with the Executive Headteacher/Head of School and/or the school's DSLs.

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

## 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the anti-bullying 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. Staff will discuss cyber-bullying with children, and the issue will be addressed in a variety of ways depending upon specific issues that need to be addressed.

Staff are also encouraged to find opportunities to use aspects of the curriculum, including Talking Points, to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see Training (Section 11) for more detail).

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 procedures set out in the school anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable strategies to ensure the incident is dealt with appropriately and necessary steps are taken to address this, including adapting future provision.

The Executive Headteacher/Head of School/DSLs will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

## 7. Acceptable use of the internet and software 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 (Acceptable use agreement EYFS/KS1 - Appendix 1, Acceptable use agreement EYFS/KS1 - Appendix 2).

For staff acceptable use agreements, please see the Acceptable Personal Use of Resources and Assets Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet and software 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 and the way that software is used by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

This monitoring is done through our Main Internet Firewall which filters unwanted content based on category, such as extremism etc... we also employ SENSO – a cloud-based Classroom Management Software that monitors computer usage on all school devices alerting Senior leaders to anything that could be classed as concerning. The software also allows for remote access support, which can be used to provide the user support to address and resolve issues.

## 8. Using devices outside school:

- **Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school and at all times adhere to our Data Handling Security Policy.

If staff have any concerns over the security of their device, they must seek advice from the IT Support Team and report any Security Incidents (actual or suspected) in line with our Security Incidents policy.

Work devices must be used solely for work activities.

- **Pupils who have been loaned devices to work on outside school**

Where appropriate, pupils are able to loan devices for the purpose of remote learning. This is agreed beforehand with SLT on a case by case basis. Pupils are expected to sign an agreement regarding the acceptable use of the school's device (Acceptable use agreement EYFS/KS1 - Appendix 3, Acceptable use agreement EYFS/KS1 - Appendix 4).

Where a device is loaned from school, a Loan Agreement is put in place and signed by the Parent / Carer and a Pupil Loan Agreement is signed by the child to confirm that they agree to take full responsibility for the device allocated to them. (Appendix 5 & 6)

These devices are provided appropriately secured and monitored via Senso, our cloud-based classroom management and monitoring solution which provides alerts to Senior Leaders should anything concerning show up.

## 9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, a DSL will investigate and log any incident using CPOMS. The action(s) taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

## 10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

All SLT members will undertake training on the use of the SENSO monitoring software and how it alerts SLT to violations and can be used to identify concerns.

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



Volunteers will receive appropriate training and updates, if applicable.

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

## **11. GDPR**

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. As a result, we are subject to greater scrutiny in our care and use of personal data.

All staff receive regular data handling awareness / data protection training and are made aware of their responsibilities.

Please see data protection policy for more information.

## **12. Monitoring arrangements**

The DSLs logs behaviour and safeguarding issues related to online safety on CPOMS

This policy will be reviewed annually by the DSLs. At every review, the policy will be shared with and ratified by the governing board.

## **13. Links with other policies**

This online safety policy is linked to our:

- Safeguarding policy and Annex 1
- Anti-bullying policy
- Staff disciplinary procedures
- Complaints policy
- Collaboration staff portable device loan agreement
- Acceptable personal use of resources and assets policy
- Data protection policy
- Collaboration security incidents policy
- Records management policy
- Data handling security policy
- Remote Learning Policy

## Appendix 1:

### EYFS / KS1 acceptable use agreement – internal (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:  
AGREEMENT FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 2:

### KS2 - acceptable use agreement - internal(pupils and parents/carers)

#### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell staff immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline

**If I bring a personal mobile phone into school:**

- I will take it to the school office for safe keeping during school hours. I will not use it during lessons.

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 3:

### EYFS / KS1 acceptable use agreement – external (Pupils & parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS OUTSIDE OF SCHOOL:  
AGREEMENT FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**When I use the school's ICT systems (like computers) and get onto the internet outside of school I will:**

- Ask an adult if I can do so before using them
- Only use websites that an adult has allowed me to use
- Tell an adult immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell an adult straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my parent/carer
- Save my work on the school systems
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and our internet when appropriately supervised by an adult. I agree to the conditions set out above for pupils using the school's ICT systems and our internet, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 4:

### KS2 - acceptable use agreement - external (Pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS OUTSIDE OF SCHOOL:  
AGREEMENT FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers) and get onto the internet outside of school I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when an adult is present, or with an adult's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my parent/carer
- Tell an adult immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless it has been assigned by school as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a parent/carer
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's ICT equipment using someone else's details
- Arrange to meet anyone offline

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer's agreement:** I agree that my child can use the school's ICT systems and our internet when appropriately supervised by an adult. I agree to the conditions set out above for pupils using the school's ICT systems and our internet, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 5:

### Pupil Portable Device Loan Agreement for parents



# Pupil Portable Device Loan Agreement For Schools within our Collaboration:



Your signature below indicates that you understand and agree to the following conditions of use:

1. I understand that all equipment loaned to my child/ren remains the property of the school and that I will need to return the equipment either when my child leaves the school or when requested to do so by a member of staff.
2. I understand that I am solely responsible for the equipment whilst it is in my child/ren's possession and I will keep the equipment in good working order, to this end if any faults should occur I agree to notify the school as soon as possible.
3. I understand that if I fail to return the IT equipment by the date stated by the school, the school reserves the right to take appropriate action to recover the IT equipment from me or to charge me for the full cost of replacing an updated version of the IT equipment.
4. I understand that this equipment is loaned to my child/ren for educational purposes and I will limit their use of this equipment to those purposes.
5. I will not sub-loan any IT equipment to others, including family members, nor will I download or install any programs not pre-approved by the school.
6. I agree that we will treat the device with care, keep the device in good condition, ensure that it is transported safely and avoid food and drink near the device.
7. I agree to follow all applicable school policies and procedures including the acceptable use policy as well as the laws regarding copyright.
8. I will repay the school for any claims made by anyone outside this Agreement for limiting their rights because of my child's use of the IT equipment. I will ensure the school is repaid for any loss or expense including legal fees which the school may receive in connection with any such claim or threatened claim by anyone outside this Agreement.
9. I agree to return this equipment for scheduled maintenance and reimaging at the request of any member of staff. I understand that reimaging may be required as a part of routine maintenance or in the event that this equipment acquires viruses, adware, spyware or malware, which will wipe the contents of the device.
10. I understand that any and all charges incurred from accessing the Internet and/or web-based services while the device is loaned to me are my responsibility and are not recoverable from the school.
11. I understand that I must not sell or otherwise dispose of the IT equipment

12. I understand that the school's insurance policy covers the device as long as the device is kept in a secure location. Should the device be lost, stolen or damaged due to not following the terms of this agreement, negligence or intentional misuse, I understand I will be liable for the full cost of replacement / repair.
13. If the laptop is stolen, I agree to contact the police immediately, inform a member of staff as well as assist the school and/or police in recovering it and complying with any investigation.
14. Should the IT equipment become lost or damaged beyond repair under the manufacturer's warranty the school will not replace it and this Agreement will come to an end.
15. The school may pause or cancel this Agreement for the loan of IT equipment if I fail in any of my responsibilities under this Agreement, the Acceptable Use Policy or I have or are reasonably suspected of Improper or illegal use of the IT equipment or if the school believes that any of these instances may occur. Where the Agreement is cancelled I will be required to return the IT equipment to the school immediately.

## Computer Make/Model:

Serial # \_\_\_\_\_ Asset Tag # \_\_\_\_\_

Loan includes:  computer  case / sleeve  battery  AC adapter/power cord  docking station  
 mouse  headset  other \_\_\_\_\_

Pupil Name(s): \_\_\_\_\_

Parent/Carer Name: \_\_\_\_\_



Parent/Carer Signature: \_\_\_\_\_ Date: \_\_\_\_\_








-----  
 -----








Return Date: \_\_\_\_\_ Checked in by: \_\_\_\_\_








(Signature of Administrator)





## Appendix 6: Pupil Portable Device Loan Agreement for children




  
 Child's agreement



 I will  look after the  laptop I  am using  and  make sure I  treat

 it with  care. I  will  tell an  adult if any  damage is done to my 

 laptop. I  will  tell an  adult if I  see any  unpleasant or  nasty

 material or  messages or anything that makes me  feel uncomfortable  online.

 Child's  Signature .....

 Date: .....