Simply Sensory
Training and Support
Creating The Building Blocks For Learning

"Live, Laugh, Learn"

SIMPLY SENSORY
ONLINE SAFETY POLICY

September 2022 - 2024

Reviewed: September 2022

Next Review Date: September 2024 (Every 2 years)

This policy is to be read in conjunction with the following policies:

- *Child Protection; Safeguarding; Managing allegations of abuse against staff;*
- *Behaviour; Anti-Bullying;*
- *Code of Conduct setting out standards and acceptable behaviour for staff;*
- *Whistleblowing;*
- *Complaints Procedure Policy and Statement;*
- *Health and Safety.*

Simply Sensory recognises UNICEF Rights and pupils are taught that they have rights and we recognise that rights and responsibilities are equally balanced and encourage our children to take responsibility for their actions in order to develop an awareness of how they affect the rights of others. Children have the right to an education that develops each child's personality and talents to the full and have a right to relax and play and join a wide range of activities. Our children are encouraged to respect their parents, each other, staff and their own and others cultures.

Simply Sensory discipline respects our children's human dignity. Every child has the right to feel safe and enjoy their education without the threat of bullying behaviour. This applies to everyone, whatever their race, religion, abilities; whatever they think or say, whatever type of family they come from.

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Simply Sensory needs to build in the use of these technologies in order to equip our young people with the skills to access life- long learning and employment.

Scope of Policy

- This policy applies to the whole of Simply Sensory including all staff employed directly or indirectly and all pupils.
- Simply Sensory will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding will be reflected within this policy.
- The Education and Inspections Act 2006 empowers senior managers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying. Sexting or other e-Safeguarding incidents covered by this policy that may take place outside of the educational environment but is clearly linked to Simply Sensory.
- Simply Sensory will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-Safeguarding behaviour that takes place out of the educational environment.

Aims and Objectives of the Policy

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the learning environment include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality.

All users need to be aware of the range of risks associated with the use of these Internet technologies. Simply Sensory understands that we have the responsibility to educate our pupils on e-safety issues, enabling them to remain both safe and legal when using the Internet and related technologies, both inside and outside the educational environment. As educators we hold personal data on learners, staff and other people to help them conduct their day-to-day activities, therefore staff need to be aware of the importance of data security.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile Internet; technologies provided by Simply Sensory (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought into educational premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media (e.g., memory stick, CD Rom) must be checked for any viruses using Simply Sensory provided anti-virus software before use.
- If you suspect there may be a virus on any Simply Sensory ICT equipment, stop using the equipment and contact the management immediately.

Data Security

The accessing and appropriate use of data is something that Simply Sensory takes very seriously.

- Simply Sensory ensures all personal data is password protected.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing Simply Sensory data.
- Staff to keep all related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it should be locked out of sight.
- Data can only be accessed on Simply Sensory computers or laptops. Staff are aware that they must not use their personal devices for accessing any Simply Sensory data.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency. This includes a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Simply Sensory

maintains a comprehensive inventory of all its ICT equipment including a record of disposal.

E-Safety

E-Safety - Roles and Responsibilities: as e-safety is an important aspect of strategic leadership within Simply Sensory, the management have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Simply Sensory Management are responsible for keeping abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

E-Safety in the Curriculum: computing and online resources are increasingly used across education. It is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within Simply Sensory and we continually look for new opportunities to promote e-safety. We provide opportunities within a range of curriculum areas to teach about e-safety:

- Educating pupils on the dangers of technologies that maybe encountered outside of education is done when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e., parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Safeguarding young people online with the view to prevent Radicalisation and Extremism.

Password security

- All users read and sign an Acceptable Use Agreement to demonstrate they have understood the E- safety Policy (App.3)
- Users are provided with an individual network, email and log in username.
- Pupils are not allowed to deliberately access online materials or files of their peers, teachers or others.
- Staff are expected to keep their passwords secret and do not share their passwords with anyone else.
- If staff or children believe their password may have been compromised, they should report it to Simply Sensory management immediately.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction as well as a potential risk to young and vulnerable people or indeed adults. Whenever any inappropriate use is detected, it will be followed up.

- Children will have supervised access to approved Internet resources at all times.
- Staff will preview any recommended sites before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Any website or social media (i.e., Facebook) that carries Simply Sensory's name is managed by Simply Sensory.

Mobile Technologies

- Staff are allowed to bring in personal mobile phones and devices for their own use. Staff should not contact pupils or parents/carers using their personal device.
- Personal mobile devices should not be visible or used during teaching time.
- Simply Sensory is not responsible for the loss, damage or theft of any personal mobile devices.
- Users bringing personal devices into the educational environment must ensure that there is no inappropriate or illegal content on the device.
- The sending of inappropriate text messages between any members of Simply Sensory community is not allowed.

Managing Email: the use of e-mail is an essential means of communication for both staff and pupils. In the context of Simply Sensory, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including: direct written contact between staff on different projects, staff based or pupil based, Pupils need to understand how to write an email in relation to their age and good network etiquette.

- Staff have their own email account to use for all Simply Sensory business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, If necessary, e-mail histories can be traced. The Sim ply Sensory email account should be the account that is used for all Simply Sensory business.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on Simply Sensory headed paper.
- Staff should actively manage their email account by deleting all emails of short-term value and organise emails into relevant folders.
- Staff and pupils must advise Simply Sensory immediately if they receive an offensive email.

Managing other Web Technologies (including Social Media): If used responsibly, social media and other web technologies both outside and within an educational context, can provide easy to use, collaborative and free facilities. We encourage our pupils and staff to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Once on the internet, words can or photos can never be erased.

- All pupils are advised to be cautious about the information given by others on sites, such as users not being who they say they are.
- Pupils are always reminded to avoid giving out personal details on such sites, which may identify them or where they are, for example: full name; address; phone number; email address.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of cyberbullying to Simply Sensory immediately.
- Staff may only create blogs, wikis or other web 2 spaces for pupils or other systems approved by Simply Sensory.
- Any social media site, such as Twitter must be managed by Simply Sensory.

Safe Use of Images

Taking of Images and Film: With the written consent of parents (on behalf of pupils) and staff, appropriate images may be taken by staff and pupils, with Simply Sensory equipment.

Publishing Pupil's Images and Work: on a child's entry to Simply Sensory, all parents/carers will be asked to give permission to use their child's work/ photos in the following ways:

- on the Simply Sensory website or social media account;
- in the Simply Sensory prospectus and other printed publications for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in internal communal areas;
- in display material that may be used in external areas, i.e., exhibition promoting Simply Sensory;
- general media appearances, e.g., local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

The consent form (Apps.1 & 2), signed by the parent/carer, is considered valid for the entire period that the child attends Simply Sensory unless there is a change in the child's circumstances where consent could be an issue, e.g., divorce of parents or custody issues. This information needs to be communicated to Simply Sensory by the parent/carer. Parents/carers may withdraw permission, in writing, at any time.

Misuse and Infringements Complaints

Complaints and/or issues relating to e-safety should be made to the Simply Sensory Management. Incidents should be logged using the e-safety incident log (App. 4).

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998: The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing. http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Telecommunications (Lawful Business Practice) Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000: Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. **http://www.legislation.gov.uk/ukpga/2000/23/contents**

Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to e-Safety

Racial and Religious Hatred Act 2006 It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003: The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Educational providers should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information http://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127): Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain access to computer files or software without permission (for example using another person's password to access files); unauthorised access, as above, in order to commit a further criminal act (such as fraud); impair the operation of a computer or program. UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1): This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988: Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29): This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1): It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964: Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997: A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data Protection Act 1998:
http://www.opsi.gov.uk/acts/acts1998/ukpga_1980029_en_1

The Freedom of Information Act 2000:
http://www.legislation.gov.uk/ukpga/2000/36/contents

Definitions of e-safety issues

The list below is not exhaustive but pertains to relevant and current e-safety issues:

Inappropriate content	It is possible that children may come across things online which are inappropriate for their age and stage of development. In school filters and restriction settings on particular devices are used to block this content.
Cyberbullying	Cyberbullying is when someone bullies others over the internet or on a mobile phone by sending abusive emails or texts directly or by posting nasty comments or humiliating images for others to see. Like any form of bullying, cyberbullying can be horrible for the children involved and hard for them to talk about.
Online grooming	Pupils may meet people online who aren't who they say they are. This could take place in a game online (Many games now are linked to the internet and players across the globe.) Grooming is a word used to describe people befriending children in order to take advantage of them for sexual purposes. Grooming usually takes place over a long period of time. In cases of sexual predators and radicalization, friendships with unsuspecting children are built up over a time span of 2-3 years.
Sexting	The term 'sexting' is used to describe the sending and receiving of sexually explicit photos, messages and video clips, by text, email or posting them on social networking sites. It's increasingly done by young people who send images and messages to their friends, partners, or even strangers they meet online.
Online reputation	The internet keeps a record of everything we do online – the photos we upload, the comments other people make about us and things we buy. This is our online reputation. It's important that children and adults understand how to manage their online reputation and the impacts for them of a negative online reputation.
Self-harm	Self-harm is often understood to be a physical response to an emotional pain of some kind, and can be very addictive. Some of the things people do are quite well known, such as cutting, burning or pinching, but there are many, many ways to hurt yourself, including abusing drugs and alcohol or having an eating disorder. People who self-harm often say it provides short-term relief to emotional pain.
Radicalisation **also known as counter-extremist narratives**	There's a chance that a child may meet people online or visit websites that could lead them over time to adopt extreme right-wing views, and become radicalised. Curiosity could lead a child to seek out these people. An adult online could befriend a child in order to encourage them to adopt beliefs or persuade them to join groups whose views and actions are considered extreme.

SEXTING POLICY

Definition of 'sexting'

Sexting is when a young person takes an indecent image of themselves and sends this to their friends or boy/girlfriends via mobile phones. There are a number of definitions of sexting but for the purposes of this advice sexting is simply defined as images or videos generated:

- by children under the age of 18, or
- of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know. The problem is that once taken and sent, the sender has lost control of these images and these images could end up anywhere. They could be seen by your child's future employers, their friends or even by child sex offenders. By having in their possession, or distributing, indecent images of a person under 18 on to someone else – young people are not even aware that they could be breaking the law as these are offences under the Sexual Offences Act 2003. (CEOP, 2015). There are many different types of sexting and it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. It is important to apply a consistent approach when dealing with an incident to help protect yourself, the school and the pupil. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All staff should be familiar with this policy.

Steps to take in the case of an incident

STEP 1: Disclosure by a student

Sexting disclosures should follow the normal safeguarding practices and protocols. A pupil is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to social services.

The following questions will help decide upon the best course of action*:*

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the child protection and safeguarding policies and practices being followed? For example, is the Designated Safeguarding Lead (DSL) for child protection on hand and is their advice and support available?
- How widely has the image been shared and is the device in the pupil's possession?
- Is it a Simply Sensory device or a personal device?
- Does the pupil need immediate support and or protection?
- Are there other pupils and or young people involved?
- Do they know where the image has ended up?

This situation will need to be handled very sensitively. Whatever the nature of the incident, ensure safeguarding and child protection policies and practices are adhered to.

STEP 2: Searching a device – what are the rules

In an educational context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a company-owned or personal device. It is important to establish the location of the image but be aware that this may be distressing for the young person involved, so be conscious of the support they may need.

The revised Education Act 2011 brought to bear significant new powers and freedoms for teachers and schools. Essentially, the Act gives schools and/or teachers the power to seize and search an electronic device if they think there is good reason for doing so. The interpretation of this Act has not yet been tested and many schools ban personal devices in schools.

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device, the following conditions should apply:

- The action is in accordance with the child protection and safeguarding policies
- The search is conducted by the Simply Sensory management or a person authorised by them
- A member of the safeguarding team is present
- The search is conducted by a member of the same sex

If any illegal images of a child are found, you should consider whether to inform the police. Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police. If an "experimental" incident is not referred to the police the reasons for this should be recorded in writing. Always put the child first. Do not search the device if this will cause additional stress to the pupil/person whose image has been distributed.

Never

- ***S***earch a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem
- Print out any material for evidence
- Move any material from one storage device to another

Always

- Inform Simply Sensory's Designated Safeguarding Lead for child protection (DSL)
- Record the incident
- Act in accordance with safeguarding and child protection policies and procedures
- Inform relevant colleagues about the alleged incident before searching a device.

If there is an indecent image of a child on a website or a social networking site, then you should report the image to the site hosting it. Under normal circumstances, you would follow the reporting procedures on the respective website. However, in the case of a sexting incident involving a child or young person where you feel that they may be at risk of abuse, then you should report the incident directly to CEOP www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

STEP 3 - What to do and not do with the image. If the image has been shared across a personal mobile device:

Always

- Confiscate and secure the device(s)

Never

- View the image unless there is a clear reason to do so (see bullet 2 above)
- Send, share or save the image anywhere
- Allow students to do any of the above

If the image has been shared across a school network, a website or a social network:

Always

- Block the network to all users and isolate the image

Never

- Send or print the image or move the material from one place to another.

STEP 4 - Who should deal with the incident?

Often, the first port of call for a pupil is a teacher. Whomever the initial disclosure is made to must act in accordance with the safeguarding and/or child protection policy, ensuring that the Designated Safeguarding Lead (DSL) and a senior member of staff are involved in dealing with the incident.

The DSL should always record the incident. Senior Management should also always be informed. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first. If viewing the image is likely to cause additional stress, professionals should make a judgement about whether or not it is appropriate to do so.

STEP 5 - Deciding on a response

There may be a multitude of reasons why a student has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

- Act in accordance with your child protection and safeguarding policy, e.g., notify DSL/SLT team
- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make a referral to LADO, if needed
- Contact the police (if appropriate)
- Put the necessary safeguards in place for the pupil, e.g., they may need counselling support, immediate protection and parents must also be informed.
- Inform parents and/or carers about the incident and how it is being managed.

STEP 6 - Contacting other agencies (making a referral)

If the nature of the incident is high-risk, consider contacting your local children's social care team. Depending on the nature of the incident and the response you may also consider contacting your local police or referring the incident to CEOP.

Monitoring and Review

The effectiveness of this policy will be monitored and evaluated by the Simply Sensory management, and will be reviewed on a bi-annual basis, with updates where necessary.

Appendix 1 - Use of Internet by Pupils

Dear Parent/Carer,

As part of the Government National Grid for Learning Scheme and to support learning opportunities with Simply Sensory, your child/children will, at appropriate times, be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet is fast becoming a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the instructor and the learner is significant and will continue to grow.

There are well publicised concerns regarding access to material on the Internet that would be unsuitable for pupils. Whilst it is impossible to ensure that a pupil will not access such material, at Simply Sensory we take all reasonable steps to minimise a pupil's access to unsuitable material. These include:

- The requirement that, wherever possible, all Internet access during educational hours will be supervised by a member of staff;
- The education of pupils as to the potential dangers and legal consequences of accessing certain types of materials.
- Attached to this letter is a copy of Simply Sensory's Policy for Acceptable Computer Use. Also included is a copy of the Rules for Safe and Responsible Use of ICT and the Internet which we would ask you to read and discuss with your child in a way you feel appropriate to their age and understanding. The Responsible ICT and Internet Use Agreement must be signed by both parent and child (where appropriate) before pupils can have access to the Internet.
- We would also ask that you sign the part of the Agreement regarding the publication of work and photographs. Usually, the pictures of children taken at school are used for display purposes, but occasionally pictures of children will appear in publications promoting Simply Sensory; these are sometimes available to the general public.
- If you wish to discuss any aspect of the Internet use or photographing the children at Simply Sensory, please telephone to arrange an appointment.

Appendix 2 - Responsible ICT and Internet Use Agreement

Pupil's Name: _____

Parent's Consent for Internet Access

I have read Rules for Responsible Use of the Internet (App 1 or 2) and give permission for my child to access the Internet. I understand that Simply Sensory will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that Simply Sensory cannot be held responsible for the nature and content of materials accessed through the Internet other than sites prescribed by staff. I agree that Simply Sensory is not liable for any damages arising from the use of the Internet facilities.

Signed: _____

Print Name: _____

Date: _____

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, child's work may be published on the Simply Sensory website. I also agree that photographs that include my child may be published and that full names will not be used.

See additional photography consent form.

Signed: _____

Print Name: _____

Date: _____

Appendix 3– Acceptable Use Agreement for Staff

ICT (including data) and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life at Simply Sensory. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Simply Sensory management.

- I will only use the Simply Sensory email for any related technologies for professional purposes or for uses deemed 'reasonable' by the Simply Sensory management.
- I will comply with the ICT system security and not disclose any passwords provided to me by Simply Sensory or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any Simply Sensory business.
- I will ensure that personal data is kept secure and is used appropriately, whether on or off educational premises or accessed remotely.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with Simply Sensory policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related media can be monitored and logged and can be made available, on request, to Simply Sensory management.
- I will support Simply Sensory's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of Simply Sensory.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in and outside Simply Sensory, will not bring my professional role into disrepute.
- I will support and promote Simply Sensory's E-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT as a member of Simply Sensory staff

Signed: _____

Print Name & Job Title: _____

Date: _____

Appendix 5 - E-Safety Incident Log

Details of ALL e-safety incidents to be recorded. This incident log will be monitored termly by the Simply Sensory management. Any incidents involving cyber-bullying may also need to be recorded elsewhere.

Date & Time	Name of pupil or staff member	Male & Female	Location/ Device	Details of Incident Including evidence	Actions and reasons