Online Safety Policy

Policy Document Status			
Date of Policy Creation	February 2023	**Chair of Governors**	Gill Stubbs
Adoption of policy by Governing Board	17 May 2023	**Executive Headteacher**	Denise Garner
Inception of new Policy	18 May 2023	**Governor/Staff Member Responsibility**	Linzi Garner
Date of policy review	April 2024	**Day Care Manager**	Shelley Thursfield

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers, and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- 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 DfE's guidance on protecting children from radicalisation.

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

The policy also considers the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Gill Stubbs**.

The Governing Board has overall strategic responsibility for online safety so they will:

- Identify and assign a member of the senior leadership team and a governor, to be responsible for ensuring effective filtering and monitoring systems.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet **(appendix 2)**
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some children with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

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

The DSL takes lead responsibility for:

- safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- working with the headteacher, computer lead and other staff, as necessary, to address any online safety issues or incidents.
- managing all online safety issues and incidents in line with the school child protection policy
- ensuring that any online safety incidents are logged either on CPOMS or **appendix 5** and dealt with appropriately in line with this policy.
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- updating and delivering staff training on online safety **appendix 4** is a self-audit for staff about online safety training needs.
- liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure children are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged **(see appendix 5)** and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet **(appendix 2),** and ensuring that children follow the school's terms on acceptable use **(appendix 1)**
- Working with the DSL to ensure that any online safety incidents are logged **(see appendix 5)** and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet **(appendix 3)**

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating children about online safety

In Early Years Foundation

Our Computing and online safety curriculum includes the youngest learners in our school and nursery settings. We plan purposeful ways for our children to create with video, photographs, digital images, sound recordings and control devices like floor robots. They also learn social skills, rules and responsible use when using devices and the internet. All of this is done with **The Characteristics of Learning** in mind, *Playing and Exploring*, *Creating and Thinking Critically*, *Active Learning*, making purposeful links to all areas of learning.

In Early Years we use stories and **Project EVOLVE** resources which provide knowledge, skills, behaviours, and attitudes over 8 strands that cover aspects of staying safe online **(see appendix 6).**

In **Key Stage 1**, children 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.

We use the **Teach Computing** Scheme **Common-Sense Media** to deliver the national curriculum and aspects relating to online safety or digital citizenship. The scheme gives teachers a clear overview of lesson objectives, an outline of the lesson and the expected outcomes **(see appendix 6).**

Each unit of work also shows links to the Education for a Connected World framework Education for a Connected World - GOV.UK (www.gov.uk)

Not all the objectives in the Education for a Connected World framework are covered in the Teach Computing Curriculum, as some are better suited to personal, social, health, and economic (PSHE) education; spiritual, moral, social, and cultural (SMSC) development. and citizenship.

All schools must teach:

- Relationships education and health education in primary schools

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some children with SEND.

5. Educating parents about online safety

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

Online safety will also be covered during parents' workshops.

The school will let parents know through the school and nursery website:

- What systems the school uses to filter and monitor online use.
  - The federation uses Telford and Wrekin ICT services who manage and monitor the filtering systems.
  - Staff use SENSO to monitor children during lessons.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying.

To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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 children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health 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 children, as part of safeguarding training (see 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 processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has

been spread among children, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices.

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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

- Assess how urgent the search is and consider the risk to other children and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

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

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

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

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

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

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

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

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

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

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

7. Acceptable use of the internet in school

- All children, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet **(appendices 1, 2 and 3).** Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by children, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.
- More information is set out in the acceptable use agreements in **appendices 1, 2 and 3.**

8. Children and Adults using mobile devices in school

- Children may not bring mobile devices into school.
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.
- Many mobile phones have access to the Internet and picture and video messaging, and such technologies present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying or inappropriate contact:
- All mobile phones will be kept in the nursery office, school office or staff cloakroom/lockers throughout contact time with pupil this includes all staff, visitors, parent helpers, supply teachers and students.
- Parents are not allowed to use their mobile on the premises. If you find a parent doing this, you should inform them of this and refer them to the Headteacher.
- Mobile phones will not be used when pupil is on the premises. However, if you have a personal emergency, you are free to use the school phone or make a personal call from your mobile in the designated staff area of the setting (Nursery office, GP room, staff room or school office.)

Staff will need to ensure that managers have up to date contact information and that staff make their families aware of emergency telephone numbers. THIS IS THE RESPONSIBILITY OF THE INDIVIDUAL STAFF MEMBER.

- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. ONLY school property can be used for this.
- Photographs and recordings can only be transferred to and stored on a school computer to be printed.
- All telephone contact with parents will be done on the school/Nursery office phone. (See exception below)
- During group outings nominated staff will have access to the school mobile, and this will be used for emergency purposes only. On trips, staff mobiles are used for emergency only.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period.
- Not sharing the device among family or friends

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in **appendix 2.**

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

11. Training

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

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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure children can recognize dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term.
-

The DSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in **appendix 5**.

This policy will be reviewed every year by the Computing Lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks children face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

13. Remote Online Learning Approach

Remote Learning will incorporate several different approaches including the use of live classes either filmed or audio. All teachers will aim to provide the best experience for children that allow feedback and interaction. They will however adopt different approaches. Teachers will use; Microsoft Teams, Purple Mash, Mathletics, Bug Club, Phonics Play, Espresso, Bitesize and The Oak Academy to support remote learning. Children will be taught how to use these safely in school.

Responsibilities while engaging in Remote Learning:

For staff and teachers:

- Teachers have overall control of the online interaction of their class. The children will wait in the lobby on Microsoft Teams and the class teacher will admit them in. When children email each other on Purple Mash teachers have control to read the emails first before they are sent to the other child.
- Teachers will do their utmost to be available at the identified time on their timetable – this may be via a Teams live video, through Teams chat, (a Collaborative workspace) or by e-mail.
- Staff will remind children of the expectations in terms of behaviour during live sessions and the conduct expected of them.
- Teachers will use the pupil's individual logins to contact on teams.
- Teachers will ensure remote learning is available for all children.
- Teachers will be aware of keeping the session as professional as possible (including checking background images on the wall, family photos in view etc.

For children:

- You are to communicate through your Purple Mash accounts with your class teacher and through live Microsoft Teams lessons.
- You must always be polite and respectful to your teachers and fellow children.
- You are not to film (by any means) or forward any content within a Microsoft Teams group – such as
- worksheets, answers, solutions, videos, notes, or links – to anyone else without the
- permission of the creator of that content.
- You understand that all your online activity is monitored. This includes anything on e-mail (Purple Mash), via
- Teams and whether you are checking regularly for assigned work.

For parents/carers:

- You should ensure that your child is checking in regularly for assigned work, registration, and lesson reviews.
- When your child is watching a live lesson, you should try to ensure your child is in an area of the
- house that is quiet and free from distractions. Be aware of background images that may be viewed and fact that other pupil should not be in the picture (to ensure safe online protocols are kept to).
- We insist that children do not try to film the session using any device.

- A live online lesson must be treated like a regular school lesson and only viewed by those who are invited to attend.

Live Online Classes:

- Children must always follow the direction of their teacher just as in the classroom.
- Children are not to film the session using any device.
- Children are not to turn on their microphone unless the teacher invites them to do so. All
- microphones should be on mute when a person is not speaking to avoid distracting background.
- noise being broadcast to everyone.
- A Teams live lesson is intended for the allocated class only. The teacher will decide who should.
- receive the invite through Teams. Only those invited by the teacher have permission to view the
- lesson.
- Staff can pre-record a lesson but must not record a live lesson.

14. Social Networking

Social networking Internet sites (such as Facebook and twitter) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact:

Use of social networking sites and newsgroups in the school is not allowed and will be blocked/filtered.

Children will be advised through online lessons never to give out personal details of any kind that may identify themselves, other children, their school, or location. This will also include not using personal photographs and videos.

Children and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged children.

Children will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

Parents, children, and staff will be advised of the dangers of discussing children, staff or the school on social networking sites. *(All staff are given guidelines in the Guide to Safer Working Practice and the T&W Social Media Policy.)* The governors will consider taking legal action, where appropriate, to protect children and staff against cyber bullying and defamatory comments.

15. Digital/ Video cameras/ Photography

Pictures, videos, and sound are not directly connected to the Internet, but images are easily transferred.

- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.

16. Email

Email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Telford and Wrekin email is used as a way to communicate between staff.
- Purple Mash is used to communicate by email to pupil during remote learning only.
- Access in school to external personal email accounts is not allowed.
- Email sent to external organizations should be carefully composed and addresses checked by another member of staff before sending, in the same way as using Microsoft Outlook.
- Chain letters, spam, advertising, and all other emails from unknown sources will be deleted without opening or forwarding.

17. Links with other policies

This online safety policy is linked to our:

- Computing Policy
- Home School Agreement
- Child Protection and Safeguarding policy
- Behaviour policy
- Staff Disciplinary Policy
- Data protection policy and Privacy Notices
- Complaints procedure

Appendix 1: EYFS and KS1 acceptable use agreement (children and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR CHILDREN AND PARENTS/CARERS	
Name of pupil:	

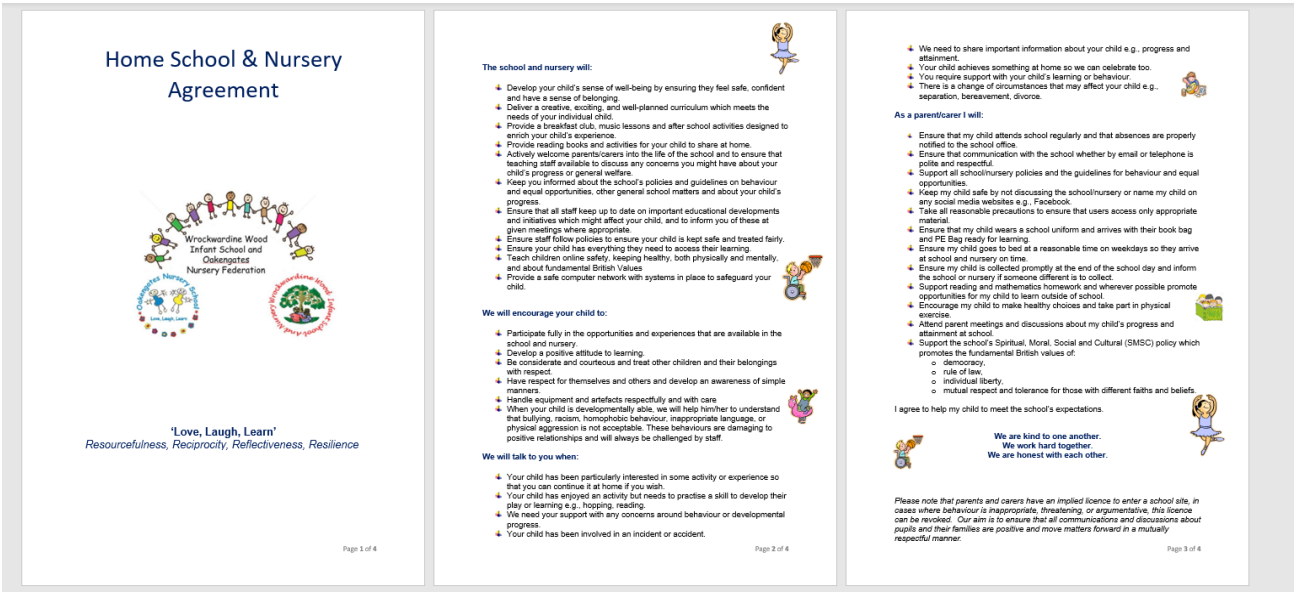
When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them.
• Only use websites that a teacher or adult has told me or allowed me to use.
• Tell my teacher immediately if:
  ○ I click on a website by mistake.
  ○ 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 schoolwork only.
• 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 children using the school's ICT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers, and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation. • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services. • Install any unauthorised software or connect unauthorised hardware or devices to the school's network. • Share my password with others or log in to the school's network using someone else's details. • Take photographs of children without checking with teachers first • Share confidential information about the school, its children or staff, or other members of the community. • Access, modify or share data I'm not authorised to access, modify or share. • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that children in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3:



Home School & Nursery Agreement

Wrockwardine Wood Infant School and Oakengates Nursery Federation

'Love, Laugh, Learn'
Resourcefulness, Reciprocity, Reflectiveness, Resilience

Page 1 of 4

The school and nursery will:

- Develop your child's sense of well-being by ensuring they feel safe, confident and have a sense of belonging.
- Deliver a creative, exciting, and well-planned curriculum which meets the needs of your individual child.
- Provide a breakfast club, music lessons and after school activities designed to enrich your child's experience.
- Provide reading books and activities for your child to share at home.
- Actively welcome parents/carers into the life of the school and to ensure that teaching staff available to discuss any concerns you might have about your child's progress or general welfare.
- Keep you informed about the school's policies and guidelines on behaviour and equal opportunities, other general school matters and about your child's progress.
- Ensure that all staff keep up to date on important educational developments and initiatives which might affect your child, and to inform you of these at given meetings where appropriate.
- Ensure staff follow policies to ensure your child is kept safe and treated fairly.
- Ensure your child has everything they need to access their learning.
- Teach children online safety, keeping healthy, both physically and mentally, and about fundamental British Values
- Provide a safe computer network with systems in place to safeguard your child.

We will encourage your child to:

- Participate fully in the opportunities and experiences that are available in the school and nursery.
- Develop a positive attitude to learning.
- Be considerate and courteous and treat other children and their belongings with respect.
- Have respect for themselves and others and develop an awareness of simple manners.
- Handle equipment and artefacts respectfully and with care
- When your child is developmentally able, we will help him/her to understand that bullying, racism, homophobic behaviour, inappropriate language, or physical aggression is not acceptable. These behaviours are damaging to positive relationships and will always be challenged by staff.

We will talk to you when:

- Your child has been particularly interested in some activity or experience so that you can continue it at home if you wish.
- Your child has enjoyed an activity but needs to practise a skill to develop their play or learning e.g., hopping, reading.
- We need your support with any concerns around behaviour or developmental progress.
- Your child has been involved in an incident or accident.

Page 2 of 4

- We need to share important information about your child e.g., progress and attainment.
- Your child achieves something at home so we can celebrate too.
- You require support with your child's learning or behaviour.
- There is a change of circumstances that may affect your child e.g., separation, bereavement, divorce.

As a parent/carer I will:

- Ensure that my child attends school regularly and that absences are properly notified to the school office.
- Ensure that communication with the school whether by email or telephone is polite and respectful.
- Support all school/nursery policies and the guidelines for behaviour and equal opportunities.
- Keep my child safe by not discussing the school/nursery or name my child on any social media websites e.g., Facebook.
- Take all reasonable precautions to ensure that users access only appropriate material.
- Ensure that my child wears a school uniform and arrives with their book bag and PE Bag ready for learning.
- Ensure my child goes to bed at a reasonable time on weekdays so they arrive at school and nursery on time.
- Ensure my child is collected promptly at the end of the school day and inform the school or nursery if someone different is to collect.
- Support reading and mathematics homework and wherever possible promote opportunities for my child to learn outside of school.
- Encourage my child to make healthy choices and take part in physical exercise.
- Attend parent meetings and discussions about my child's progress and attainment at school.
- Support the school's Spiritual, Moral, Social and Cultural (SMSC) policy which promotes the fundamental British values of:
  - democracy,
  - rule of law,
  - individual liberty,
  - mutual respect and tolerance for those with different faiths and beliefs.

I agree to help my child to meet the school's expectations.

We are kind to one another.
We work hard together.
We are honest with each other.

Please note that parents and carers have an implied licence to enter a school site, in cases where behaviour is inappropriate, threatening, or argumentative, this licence can be revoked. Our aim is to ensure that all communications and discussions about pupils and their families are positive and move matters forward in a mutually respectful manner.

Page 3 of 4

Children will:

- always behave well, including on social media
- keep the school expectations.
  - We are kind to each other.
  - We are honest with each other.
  - We work hard together.
- accept responsibility for the choices they make.
- listen carefully and be attentive in lessons.
- complete homework and take home their reading book.
- look after each other and respect other children's culture, race, feelings, beliefs, and values.
- be polite and kind to all members of the school community.
- tell a member of staff if they are worried or unhappy.
- follow advice from online safety lessons.

Signature:	Headteacher
Signature:	Parents/Carers
Signature:	Child
Date:	

Page 4 of 4

Appendix 4 online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways children can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for children and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 6: Online Safety lessons in the EYFS and KS1

Nursery	1st Half term	2nd Half Term
Autumn	**Digital Literacy- Online safety -** Seeks to acquire basic skills in turning on and operating some ICT equipment. **Computer Science-** Operates mechanical toys, e.g., turns the knob on a windup toy or pulls back on a friction car**.** Technology hunts and what toys need to operate. Can you operate some ICT equipment? **IT-** Shows an interest in technological toys with knobs and pulleys, or real objects such as cameras or mobile phones. Shows skill in making toys work by pressing parts or lifting flaps to achieve effects such as sound, movement, or new images. Control the kettle, microwave, and toaster. **IT available in continuous provision** Roleplay -kettle, toaster, microwave Lightbox Laptops Large IWB screen (Beep Beep, phase 1 early literacy) CD player	**Digital Literacy—Online Safety** Netsmartz - Router's birthday surprise **Computer Science-** Knows how to operate simple equipment e.g., turns the CD player on and uses a remote control. Children explore programmable toys. Cars, cats **IT available in continuous provision** Roleplay -kettle, toaster, microwave Lightbox Laptops Large IWB screen (Beep Beep, phase 1 early literacy) CD player
Spring	**Digital Literacy—Online Safety** Smartie the penguin - eBook **IT-** Knows how to operate simple equipment e.g., turns the CD player on and uses a remote control. knows that information can be retrieved from computers. To use the cd player, play, pause, stop, sound, headphones. Children learn you can find out information on an iPad/computer. **IT available in continuous provision** Roleplay -kettle, toaster, microwave Lightbox Laptops Large IWB screen (Beep, Beep, phase 1 early literacy) CD player	**Digital Literacy—Online Safety** Chicken clicking story book **Computer Science -** Knows how to operate simple equipment e.g. turns the CD player on and uses a remote control**.** To control a programmable toys car, cats and complete an obstacle course. Children use the language forward, backwards and turn. **IT available in continuous provision** Roleplay -kettle, toaster, microwave Lightbox Laptops Large IWB screen (beep beep, phase 1 early literacy) CD player

Love, Laugh, Learn'

Resourcefulness, Resilience, Reciprocity, Reflectiveness

Summer	**Digital Literacy—Online Safety** Netsmartz - delivery for Webster **IT-** knows that information can be retrieved from computers. Completes a simple program on the computer. Complete a simple program on the computer. Children learn to take a picture of tuff cam. Children learn you can find out information on an iPad/computer. **IT available in continuous provision** Roleplay -kettle, toaster, microwave Lightbox Laptops Large IWB screen (beep, beep, phase 1 early literacy) CD player	**Digital Literacy—Online Safety** Digi duck story: learn that staying safe online is like staying safe in the real world. **IT- Completes a simple program on the computer.** To begin to use a computer mouse and not just touch screen. **Computer Science -** Uses ICT hardware to interact with age-appropriate computer software. Give a simple instruction to Cubetto. Use the language, forward. **IT available in continuous provision** Roleplay -kettle, toaster, microwave Lightbox Laptops Large IWB screen (beep, beep, phase 1 early literacy) CD player

Love, Laugh, Learn'

Resourcefulness, Resilience, Reciprocity, Reflectiveness

Reception	1st Half term	2nd Half Term
Autumn	**Digital Literacy—Online Safety** Smartie the penguin - eBook Project evolve-When and What: Managing Online Information **Computer Science** On/Off Button-Hello Ruby **Computational Thinking** Pumpkin Soup-Link to Harvest -Barefoot Resources **IT** Technology safari- Hello Ruby (Link with **Project Evolve**: I can recognise some ways in which the internet can be used to communicate.: Online Relationships) **IT available in continuous provision** Use a computer mouse. To complete a simple program. (Early literacy, Beep Beep, Phonics play, Purple Mash, mathematics games) Use a digital camera on Autumn walk. Roleplay toaster, microwave	**Digital Literacy—Online Safety** Netsmartz - Router's birthday surprise **Computer Science-** Me and the computer-Hello Ruby **Project Evolve** PowerPoint: which rules are fair: Health, Well-being, and Lifestyle **Computational Thinking** Winter warmers snowmen and scarves **IT available in continuous provision** Use a computer mouse. To complete a simple program. (Early literacy, Beep Beep, Phonics play, Purple Mash, Maths games) Video camera Christmas play Roleplay toaster, microwave
Spring	**Digital Literacy—Online Safety** Jessie and Friends (Think you know) Linked to online safety day. Project evolve: Stomp your feet, spot the difference: Online Bullying Use Project evolve sayings: Responses and Reactions: Self-Image and Identity **Computer Science** Remote Control-Hello Ruby **Project Evolve** sentence starters: what are your rules? Health, Well-being, and Lifestyle Explore the ozobots **Computational Thinking** Feed the birds-Barefoot Computing (Link with the big bird watch) **IT available in continuous provision** To create a picture and use basic drawing tools. **Project Evolve** activity: Guess the file: Copy wright and ownership. Use a digital camera on Winter walk.	**Digital Literacy—Online Safety** Chicken Clicking story book. **Computer Science** Toothbrush algorithm- Hello Ruby (Link to jigsaw healthy me) **Computational Thinking** Springtime seeds- Barefoot Computing (links with science) **IT available in continuous provision** To create a picture and use basic drawing tools. To type their name on the computer. **Project Evolve**: whose is this? copy wright and ownership activity: Use a digital camera on Spring walk.

Love, Laugh, Learn'

Resourcefulness, Resilience, Reciprocity, Reflectiveness

Summer	**Digital Literacy—Online Safety** Digi duck's big decision **Project Evolve:** keep me informed: Online Reputation **Computer Science** Children explore the Cubetto programmable toys. Move forwards, backwards. **Computational Thinking** Rabbit Run-Barefoot Computing **IT available in continuous provision** To create a picture and use basic drawing tools. To type their name on the computer. Use a digital camera to take pictures of plants.	**Digital Literacy—Online Safety** Hectors World- Personal Information learn that staying safe online is like staying safe in the real world. **Project Evolve** PowerPoint: Personal or private: Privacy and Security **Computer Science** My first computer-Hello Ruby Children explore the Cubetto programmable toys. Move forwards, backwards, left, and right. **Computational Thinking** Seaside Tangrams-Barefoot Computing **IT available in continuous provision** To create a picture and use basic drawing tools. To type their name on the computer. Use a digital camera to take pictures on summer walk. To become aware of a pictogram to collect information linked to Design and Technology favourite fruit.

Love, Laugh, Learn'

Resourcefulness, Resilience, Reciprocity, Reflectiveness

Year 1	1st Half term	2nd Half Term
Autumn unit	**Digital Literacy—Online Safety** Keep it private (Common sense media planning) **IT-**Technology around us	**Digital Literacy—Online Safety** ABC searching (Common sense media planning) **IT-**Digital Painting
Spring unit	**Digital Literacy—Online Safety** E-Safety Day theme (Computing lead will share planning) **Computer Science -**Moving a robot	**Digital Literacy—Online Safety** Going places safely (Common sense media planning) **IT-**Grouping Data/Online Safety
Summer unit	**Digital Literacy—Online Safety** My creative work (See Common sense media planning) **IT-**Digital Writing/Online Safety	**Digital Literacy—Online Safety** Sending Email (See Common sense media planning) **Computer Science -**Introduction to animation

Year 2	1st Half term	2nd Half Term
Autumn unit	**Digital Literacy—Online Safety** Staying safe online (Common sense media planning) **IT** Information technology around us/Online Safety	**Digital Literacy—Online Safety** Follow the Digital Trail (Common sense media planning) **IT-**Digital Photography
Spring unit	**Digital Literacy—Online Safety** E-safety Day (Computing Lead to send planning) Use technology safely and respectfully, keeping personal information private. **Computer Science** Robot algorithms	**Digital Literacy—Online Safety** Screen out the Mean. Introduction to cyberbullying (See Common Sense Media). **IT-**Pictograms/Online Safety
Summer unit	**Digital Literacy—Online Safety** Using Keywords (See Common sense media planning) **IT-**Making music/online Safety	**Digital Literacy—Online Safety** Sites I like (See common sense media planning) **Computer Science-**Introduction to quizzes