Herne CE Infant and Nursery School Online Safety policy

Our school family: learning, loving and growing together rooted in God's love'

All stakeholders demonstrate the school Christian values ensuring that they act in accordance to this policy. As Stewards of God's creation we are entrusted to ensure the Health and safety of our children, staff and families.

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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 Head of School/Exec Heads and school staff
- Relationships and sex education (RSE) and health 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Head of School/Exec Head to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs. The governor who oversees online safety is Dr Elizabeth Thundow

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Head of School/Exec Head

The Head of School/Exec Head is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

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

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

- making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with Leaders and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT technician (SNS) to make sure the appropriate systems and processes are in place
- Working with the Head of School/Exec Head, ICT manager 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see Appendix 3 and CPOMs if related to child) and dealt with appropriately in line with this policy
- Making sure 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT Technician (SNS – external IT support)

The ICT technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see Appendix 3 and CPOMs if related to child) and dealt with appropriately in line with this policy
- Making sure 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 making sure that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting DSL and completing a report.
- Following the correct procedures by requesting permission from the Head of School/Exec Head and ICT Technician if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see Appendix 3 and CPOMs if related to child) and dealt with appropriately in line with this policy
- Making sure 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/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of School/Exec Head of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1) Parents indicate their agreement of this document using Arbor permissions.

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

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 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

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 pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

Online safety will also be covered during parents workshops, newsletters and events.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access.

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

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand why it is important to stay safe online and how they can protect themselves online.

We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will discuss cyber-bullying with pupils in an age appropriate way linked to keeping themselves safe online.

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 pupils, as part of safeguarding training (see section 11 for more detail).

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

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

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

6.3 Examining electronic devices

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

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head of School/Exec Head
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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 DSL / Head of School/Exec Head 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 whether 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/carer 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 pupils will be carried out in line with:

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

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Herne CE Infant and Nursery School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone’s likeness.

Herne CE Infant and Nursery School will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 to 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils are not permitted to bring mobile devices into school. Should this be suspected staff will remove and inform parents. The DSL/HoS/Exec Head will decide if it is necessary to investigate if it has been used in school and follow appropriate actions as set out in 6.3.

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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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 of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that 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 ICT support 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 on behaviour and ICT and internet acceptable use. 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 code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

11.1 Staff, governors and volunteers

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, threatening, 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies 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 on the subject of 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.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 3 (and CPOMs if related to child).

This policy will be reviewed annually. 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 pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Reviewed Sept 2025
Next review Sept 2026

Signed …….. Date ……
(Chair of Governors)

Signed …….. Date …….
(Head of school)

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

Pupils Acceptable Use Policy

EYFS and KS1 Statements

- I only go online with a grown up when I am using the computers, I-pads or the interactive whiteboards in school
- I only click on links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I have talked about these rules at home

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can only click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always tell a grown up if something online makes us feel unhappy or worried.

We keep information about ourselves safe and don't share it with people we don't know.

We can only send messages online which are polite and friendly.

Parents/Carers Acceptable Use Policy Statements

1. I have read and discussed the Pupil Acceptable Use Policy with my child.
2. I know that my child will receive Online Safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation.
4. I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
5. I understand that if my child discovers, discusses or seeks unsafe material on-line in school, immediate advice will be sought and parents informed.
6. I, together with my child, will support the school's approach to Online Safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
7. I know that I can speak to the school Designated Safeguarding Lead, Miss Lucy St John, my child's teacher or the Executive Head Teacher if I have any concerns about Online Safety
8. I will visit the school website www.herne-infant.kent.sch.uk for more information about the school's approach to Online Safety as well as to access useful links to support both myself and my child in keeping safe online at home
9. I will visit the following websites for more information about keeping my child safe online
    - www.thinkuknow.co.uk/parents,
    - www.nspcc.org.uk/onlinesafety
    - www.internetmatters.org
    - www.saferinternet.org.uk
    - www.childnet.com
10. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home

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

Staff Acceptable Use Policy

As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Head of School. Activities such as buying or selling goods are inappropriate.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager. I will use a 'strong' password; a strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly.
- I will not reveal my home address, telephone number, school name, or picture to people I meet on the Internet.
- I am aware that when using a school laptop on a home internet, I am not protected by school filtering systems and therefore could contravene the school Systems Code of Conduct.
- I will not install any software or hardware without permission.
- I will check any files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- I will not connect any mobile equipment (e.g. laptops, tablet PCs etc.) to the school network without first seeking permission of the systems Manager.
- I understand that School Laptops are to be returned to school three times a year for checking and updating or when requested by the school systems manager.
- I will protect the computers from spillages by eating or drinking well away from the IT equipment.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018.
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

- Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
- Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep or access professional documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment (KLZ) or via VPN.
- I will respect copyright and intellectual property rights.
- I will only open attachments to emails if they come from someone I already know and trust. I understand that attachments can contain viruses or other programs that could destroy all the files and software on my computer & network.
- I understand that the sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead (Lucy StJohn) as soon as possible.
- I will ensure that any electronic communications are compatible with my professional role by being polite and appreciating other users might have different views from my own. I also understand the use of strong language, swearing or aggressive behaviour is not acceptable.
- I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I understand that the school may exercise its right to monitor the use of ~~i~~information systems, including internet access and the interception of emails, in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.
- I understand that my use of the school information systems, including any devices provided by the school, school internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: ……..…… Date: ……

Accepted for school: ……Capitals: ……... Date: ……

Appendix 3: 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**