**Acceptable Use Policy and Inhouse Audit Tool**

**Wickselm House aims to:**

* Have robust processes in place to ensure the online safety of children, staff, volunteers and contractors.
* Deliver an effective approach to online safety, which empowers us to protect and educate the whole setting 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, anti-Semitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as child-to-child 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.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

**Legislation and guidance**

This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (2024), and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff 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.

**Roles and responsibilities**

The setting lead

Hannah O’Brien is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the setting.

The Designated Safeguarding Lead

* Details of the setting’s DSL and deputies are set out in our Safeguarding & Child Protection policy. The DSL takes lead responsibility for online safety in setting, in particular:
* Supporting staff to understand this policy and that it is being implemented consistently throughout the setting.
* Managing all online safety issues and incidents in line with the setting’s Child Protection Policy
* Ensuring that any online safety incidents are logged (see appendix 3) 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 setting’s Behaviour Policy
* Updating and delivering / organising staff training on online safety
* Liaising with other agencies and/or external services if necessary

The SLT are 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 Wickselm House, including terrorist and extremist material.
* Ensuring that the setting’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
* Supporting the Online Safety Auditor to conduct a full security check and monitoring the setting’s ICT systems on a regular 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 3) and dealt with appropriately in line with this policy.
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the setting’s Behaviour Policy.
* This list is not exhaustive.

All staff and volunteers

All staff, including contractors, 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 setting’s ICT systems and the internet (appendix 2), and ensuring that children follow the setting’s terms on acceptable use (appendix 1)
* Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy.
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the setting’s 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 exhaustive.

Parents

Parents are expected to:

* Notify a member of staff or the manager of any concerns or queries regarding this policy.
* Ensure their child has read, understood and agreed to the terms on acceptable use of the setting’s ICT systems and internet (appendix 1)
* 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 Healthy relationships
* Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the setting’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 2).

Educating children about online safety

Children will be taught about online safety as part of the curriculum and where appropriate to their level of understanding and development.

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.
* Recognise acceptable and unacceptable behaviour.
* Identify a range of ways to report concerns about content and who they can report their concerns to.

By the end of their journey with us, children will know:

* That people sometimes behave differently online, including by pretending to be someone they are not.
* That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
* The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
* How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
* How information and data is shared and used online.
* What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
* How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
* 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.

**Educating parents about online safety**

The setting will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website.

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

**Cyber-bullying**

Definition:

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

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.

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

In relation to a specific incident of cyber-bullying, the setting will follow the processes set out in the setting’s Anti Bullying Policy. Where illegal, inappropriate or harmful material has been spread among children, the setting will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

**Examining electronic devices**

Staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on childrens’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

• Cause harm, and/or

• Disrupt and/or break any of the setting rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

• Delete that material, or

• Retain it as evidence (of a criminal offence or a breach of school discipline),

• and/or report it to the police\*

\* Staff may also confiscate devices for evidence to hand to the police, if a child discloses that they are being abused and that this abuse includes an online element.

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

• The DfE’s latest guidance on screening, searching and confiscation.

• UKCIS guidance on sharing nudes and semi-nudes.

• Advice for settings working with children and young people.

• The setting’s COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on childrens’ electronic devices will be dealt with through the setting’s Complaints Policy.

**Acceptable use of the internet in the setting**

All children, parents, staff, volunteers are expected to sign an agreement regarding the acceptable use of the settings ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the setting’s terms on acceptable use if relevant.

Use of the setting’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, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

**Staff using work devices outside setting**

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)
* Making sure the device is locked if left inactive for a period of time
* Not sharing the device among family or friends
* Staff members must not use the device in any way which would violate the setting’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 school ICT provider.

**How the setting will respond to issues of misuse**

Where a child misuses the setting’s ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and 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 setting’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 and staff behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

**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 other children 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 recognise dangers and risks in online activity and can weigh the risks up.
* 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 and deputies will undertake Child Protection and Safeguarding training, which will include online safety, at least every 3 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding & Child Protection Policy.

**Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year and 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.

**Links with other policies**

This Acceptable Use Policy is linked to our: Safeguarding & Child Protection Policy, Behaviour Policy, Staff Behaviour & Disciplinary Policy, GDPR & Privacy Policy, Complaints Policy and E-Safety Policy.

**Appendix 1: Acceptable use agreement (children and parents/carers)**

**Name of child:**

**When I use the setting’s ICT systems (like computers) and use the internet I will:**

Ask a member of staff if I can do so before using them

Only use websites that a member of staff has told me or allowed me to use

Tell a member of staff 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

**I will:**

* Use Wickselm computers for Wickselm activities only
* Be kind to others and not upset or be rude to them
* Look after Wickselm’s ICT equipment and tell an adult straight away if something is broken or not working properly
* Never share my password (if I have one) with anyone, including my friends.
* Never give my personal information (my name, address or telephone numbers) to anyone without the permission of a member of staff or parent/carer
* Save my work on the Wickselm network
* Check with a member of staff before I print anything
* Log off or shut down a computer when I have finished using it

I agree that Wickselm staff will monitor the websites I visit and that there will be consequences if I don’t follow the rules.

Signed (child): Date:

Parent/carer agreement: I agree that my child can use the setting’s ICT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for children using the setting’s ICT systems and internet and will make sure my child understands these.

Signed (parent/carer): Date:

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

**Name of staff member/volunteer/visitor:**

When using the setting’s ICT systems and accessing the internet at Wickselm, or outside of Wickselm 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 setting’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 setting’s network

• Share my password with others or log into the setting’s network using someone else’s details

• Take photographs of children without checking with the setting lead first

• Share confidential information about the setting, 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 setting

I will only use the setting’s ICT systems and access the internet at Wickselm, or outside of Wickselm on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that Wickselm will monitor the websites I visit and my use of its ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside of the setting, and keep all data securely stored in accordance with this policy and the setting’s GDPR policy.

I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a child 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 setting’s ICT systems and internet responsibly and ensure that children in my care do so too.

Signed (staff member/volunteer/visitor): 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