The Whiteoak Academies of Hannah More Infant and Grove Junior Schools

Planting Dreams, Nurturing Hearts, Growing Minds

Online Safety Policy

Contents

C11 Online Safety & Technical Security Policy 2023-24

1. Aims and Rationale

Our school aims to:

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

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school, especially with the recent need for home learning. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school online safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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](#)
- [Cyber-bullying: advice for Headteacher and school staff](#)

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

The local governing board will receive regular information including incidents and will monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy.
- Adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).

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. **The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community**, though certain day-to-day responsibilities for online safety will be delegated to the *Designated Safeguarding Leader (DSL), Computing Online Safety Leader, Computing and Online Safety support staff and ICT Technician.*

The Headteacher is responsible for ensuring that the DSL*,* Computing Online Safety Leader and ICT technician and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding leaders (DSL) are set out in our safeguarding policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (using CPOMS) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged (using CPOMS) 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 Headteacher and/or governing body.

C11 Online Safety & Technical Security Policy 2023-24

3.4 The Computing Online Safety Leader

The computing online safety leader is responsible for:

- Putting in place appropriate filtering and monitoring systems with the ICT Technician, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

- Work with the ICT technician to ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

- Ensure use of SWGfL to ensure blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. Ensuring that any online safety incidents are logged (using CPOMS) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of online safety (using CPOMS) and dealt with appropriately in line with the school behaviour policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Take the day-to-day responsibility for online safety issues and reviews and they monitor this policy, regularly updating the policy to meet the school's needs.

- Provide appropriate training and advice for staff.

- Regularly inform the Headteacher, the DSL, ICT technician and governors of online safety incidents.

This list is not intended to be exhaustive

3.5 The ICT Technician

The ICT Technician is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

- That the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority/LSP Online safety Policy and guidance.

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- That users may only access the school's networks with properly enforced password protection, in which passwords are regularly changed.

- SWGfL is informed of issues relating to the filtering applied by them.

- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- That the use of the *network / remote access / email* is regularly monitored in order that any misuse or attempted misuse can be reported to the *Online Safety Lead/ Headteacher for investigation.*

- That monitoring software / systems are implemented and updated as agreed in school policies.

3.6 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, and ensuring that pupils follow the school's terms on acceptable use.

- Working with the DSL to ensure that any online safety incidents are logged (using CPOMS) 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 and logged (using CPOMS).

- Ensuring online safety issues are embedded in all aspects of the curriculum and other school activities.

- Ensuring pupils understand and follow the school online safety and acceptable use policy.

- Ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

- In lessons, where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.7 Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.*

 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 and understood the expectations and the terms on acceptable use of the school's ICT systems and internet when learning at school or at home (appendix 1).

- 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 and recorded on CPOMS.

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

3.8 Pupils

- Pupils are expected to follow the school rules of **'Ready, Respectful, Safe'** at all times when learning at school or at home.
- Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use expectations (appendix 1) when learning at school and at home. When learning at home, in addition to the acceptable use expectations, they are to adhere to the remote learning guidance (appendix 2).

- Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Pupils will be expected to follow the Acceptable Users Policy on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

- Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

- Through the teaching of the school's Computing curriculum and PSHE curriculum, pupils will be taught the importance of online safety.

3.9 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 adhere to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

4.1 The curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating to take a responsible approach. The education of *pupils* in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

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

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

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

- • Use technology safely, respectfully and responsibly.
- • Recognise acceptable and unacceptable behaviour.
- • Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- • That people sometimes behave differently online, including by pretending to be someone they are not
- • That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- • The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

The school will use resources from National Online Safety to deliver a comprehensive and progressive scheme from Reception to Year 6. See Appendix for the focus of lessons for each term.

Online safety, including the safe use of social media and the internet, will also be covered in other subjects where relevant including PSHE and class assemblies. The profile of online safety will also be raised through online safety day.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Pupils should be helped to understand the need for the pupil engagement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5. Educating parents about online safety

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

The school will let parents 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 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 one 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 what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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.

The school also sends information/newsletters/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 and anti-bullying policies. 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 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.

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 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 Headteacher/DSL. Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

- 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 staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team 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 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

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

7. Acceptable use of the internet in school

All staff, and volunteers are expected adhere to the acceptable use of the school's ICT systems and the internet (appendices 1, 2 and 3) for learning at school and at home. Visitors will be expected to read and adhere 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.

More information is set out in the acceptable use expectations in appendices 1, 2 and 3.

8. Using mobile devices and photo/video devices in school

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should

only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media and printed publications.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Pupils are not permitted to bring mobile phones into school unless a valid need has been approved by SLT. Parents of Year 5 and 6 children, who wish their child to bring a mobile phone to school, will be asked to complete a Mobile Phone Permission Form. This will be reviewed by SLT. Children who have been granted permission will need to present their switched off phone to the class teacher on arrival at school where it will be stored in a lockbox for the duration of school and returned at the end of the day.

Any breach of the mobile phone permission contract by a pupil may trigger disciplinary action in line with the school behaviour policy and will result in the immediate confiscation of their device and permission being withdrawn.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be used safely and securely.

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

Work devices must only be used for work activities.

10. How the school will respond to issues of misuse

Our IT support company regularly updates the DSL is children/ staff have made searches for concerning items or attempted to access inappropriate sites.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. 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. 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.

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images

- adult material which potentially breaches the Obscene Publications Act

- criminally racist material

- Other criminal conduct, activity or materials.

The SWGfL flow chart below and https://swgfl.org.uk/onlinonline safety/ can be used to advise on actions.
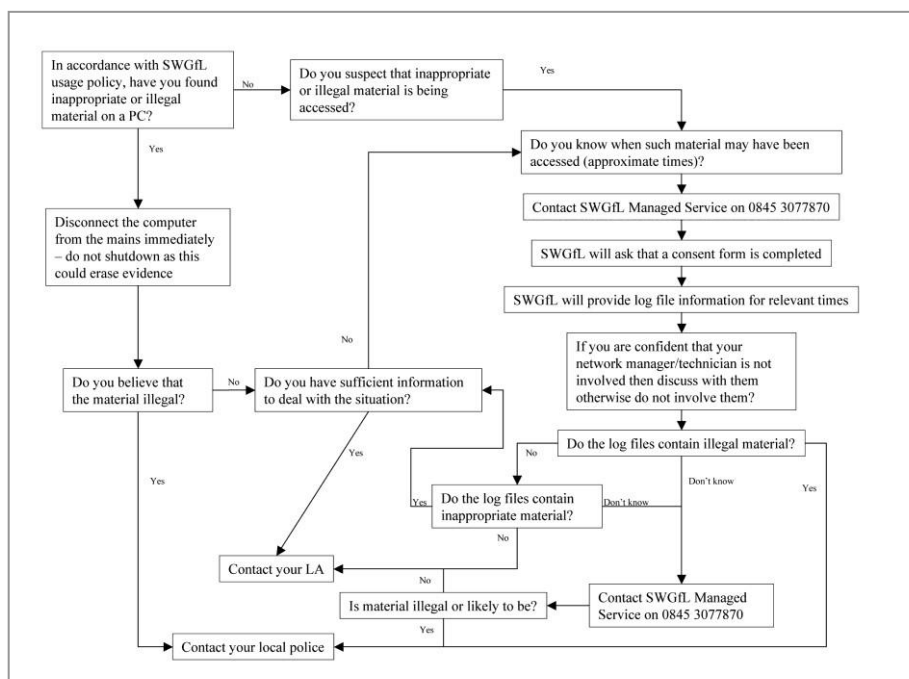
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

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:

C11 Online Safety & Technical Security Policy 2023-24

- 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the online safety lead. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- LSP Safeguarding policy

- Behaviour policy

- Anti-bullying policy

- LSP Staff disciplinary procedures

- LSP Data protection policy related to GDPR and privacy notices

- LSP Complaints procedure

C11 Online Safety & Technical Security Policy 2023-24

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

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

Name of pupil:

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

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

Signed (pupil):	**Date:**

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

Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

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

Name of pupil:

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

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

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

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

Signed (pupil):	**Date:**

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

Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS 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 pupils without checking with teachers first
- Share confidential information about the school, its pupils 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 pupils in my care do so too.

Signed (staff member/governor/visitor):	**Date:**

Appendix 4: Long term plan for online safety curriculum.

Online Safety Curriculum at
The Whiteoak Academies

Term	Focus
1	Online relationships
2	Health, wellbeing and lifestyle Online Bullying
3	Privacy and Security
4	Self-image and identity Copyright and ownership
5	Managing Online Information
6	Online reputation