Online Safety Policy

Ownership:	Governing Body
Date of Issue:	September 2022
Review Date:	September 2023
Headteacher:	Debbie Miller
Signature:	Mrs D Miller
Date:	September 2022
Chair of Governors:	Judith Sparks
Signature:	Mrs J Sparks
Date:	November 2022

Wheatcroft Primary School, Stanstead Road, Hertford, Hertfordshire, SG13 7HQ

Tel: 01992 587899 **Email:** admin@wheatcroft.herts.sch.uk

Introduction

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

Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. At Wheatcroft, we understand the responsibility to educate our pupils on Online Safety Issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Aims and objectives

In addition to our aims for Computing, the school aims to:

- Develop all pupils' positive attitude towards Online Safety, and develop an understanding of the appropriate use of technology.
- Provide a safe environment for the use of ICT and teach safe use for all staff and pupils.

Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education ,GDPR, health and safety, home–school agreement, behaviour, anti-bullying and PSHE/RSE policies.

Subject leadership and coordination

The class teacher, Key Stage Leads and the Computing Subject Leader will share responsibility for the delivery of the curriculum. The Computing Subject Leader will oversee planning, assessment and resources. Monitoring of standards and practice across the school will normally be achieved through the Subject Leader's evaluation of Computing lessons and planning across the whole school in conjunction with the Headteacher and Leadership team. The Subject Leader will assess samples of work from all classes and feedback findings. Assessment is to be completed at end of term intervals by class teachers to monitor progress.

The Subject Leader will ensure that colleagues are informed of any new developments in the subject or given relevant information received on Professional Development courses or briefings. Staff will be encouraged to discuss their ideas and/or difficulties with the Subject Leader or Phase Leader. With support from the Leadership Team, the Subject Leader will identify the needs for staff development.

The Subject Leader is responsible for:

- identifying the needs of the school in Computing;
- monitoring the quality of teaching and learning in Computing;
- monitoring planning for Computing;
- monitoring and tracking data in Computing;
- the ordering, storage and maintenance of resources;
- developing and implementing policies;
- maintaining a current Subject Leader Action Plan to inform school development.

Curriculum delivery

When planning, teachers use a variety of different materials in conjunction with the National Curriculum, Early Years Foundation State Framework and Herts for Learning Computing Scheme.

We use our school long-term curriculum planning to guide our teaching. As we have some mixed year groups, we follow a two year cycle in our planning to ensure coverage (See Appendix A), with support from materials from Herts for Learning (HfL). In our medium-term planning, we set out the aims, objectives and success criteria giving details of what is to be taught to each year group. We identify opportunities for assessment within each unit of work. Lessons are planned with clear learning objectives, which are based upon the teacher's detailed knowledge of each child. We strive to ensure that all tasks are appropriate to each child's level of ability, including provision for children on the SEN (Special Educational Needs) and MAGT (More Able, Gifted and Talented) registers.

Online safety is embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE and RSE curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge. It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk. The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school-approved accounts on the school system for educational purposes. Where required, parent/carer permission will be obtained for the pupil accounts to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Security and GDPR Policies. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to a member of SLT or Computing Lead.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content.
- When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
  - Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
  - Adult material that breaches the Obscene Publications Act in the UK
  - Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
  - Promoting hatred against any individual or group from the protected characteristics above
  - Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
  - Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence,gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitored system has been set up by the school for use on a personal device; such a system would ensure the user was not saving files locally to their own device and breaching data security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Head Teacher.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).
Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by Head Teacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement (Appendix A) and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils must only use school equipment to record images of pupils whether on or off site. Please refer to the GDPR and Data Security Policies for more detail.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Members of staff may only use a personal device to contact a pupil or parent if given permission by the Headteacher i.e. pandemic, off site visit with strict rules of withholding the phone number.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Head Teacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times, all such devices must be switched off and handed into their class teacher where they will be kept safely until the child goes home. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Personal mobiles must never be used to access school emails and data, unless permission given by Headteacher in emergencies i.e. COVID/Pandemic, Off Site on a trip. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the Computing Lead before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSP, the headteacher or Computing Lead and the incident recorded on CPOMS. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.
It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.
All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.
The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.
Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Resources for Staff/Parents

Bullying
www.bullying.co.uk - One in five young people have experienced bullying by text message or via email. This web site gives advice for children and parents on bullying.
CBBC
http://www.bbc.co.uk/cbbc/topics/stay-safe - The CBBC website has a 'stay safe' area for primary children and has a cartoon and quiz.
Child Exploitation and Online Protection (CEOP) Centre
www.ceop.gov.uk - The Child Exploitation and Online Protection (CEOP) Centre works across the UK and maximises international links to deliver a holistic approach that combines police powers with the dedicated expertise of business sectors, government, specialist charities and other interested organisations - all focused on tackling child sex abuse wherever and whenever it happens. Links to Cyber Café and Hector's World.
Childnet
www.childnet.com **-** *A non-profit making organisation working directly with children, parents and teachers to ensure that the issues of online child protection and children's safe and positive use of the internet are addressed. Childnet International produces an online CD guide specifically for parents KnowITAll - http://www.childnet.com/resources/kia/*
Children and new technology- the Byronreview
www.dfes.gov.uk/byronreview/ - Safer Children in the Digital World, independent review for the Government looking at the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games.
Digizen
www.digizen.org/ - in connection with Childnet, this site provides information on cyberbullying and social networking.
European Internet Safety Resource
www.saferinternet.org - Promotes internet safety in Europe with a regular newsletter. Articles on safe use of the internet, mobile phones, gaming, chat rooms by children. Covers what to do about illegal content and harmful content.
Get Safe Online
www.getsafeonline.org - A Government sponsored one-stop-shop for reliable, up-to-date information about online safety, to give home users and small businesses the advice they need to use the Internet safely.
_Hertfordshire Police
https://www.herts.police.uk/advice/chatright_-_internet_safety.aspx **-** e-Safety advice from Hertfordshire police, including downloadable materials
Herts Grid for Learning
http://www.thegrid.org.uk/eservices/safety/ - Link to the Hertfordshire Grid for Learning e-Safety advice. Includes powerpoints on e-Safety and lists of useful web pages.
Kidsmart
www.kidsmart.org.uk - Kidsmart is an award winning practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Childnet International.
London Grid for Learning
http://www.lgfl.net/esafety/Pages/safeguarding.aspx - Resources, web links and downloadables aimed at school staff.
Teachers TV
https://www.tes.com/teaching-resource/teachers-tv-ks3-4-ict--online-safety-6039010
This programme outlines simple classroom activities to help teachers to take practical steps to keep pupils safe online and to increase awareness of the potential dangers of internet usage.
Thinkuknow
www.thinkuknow.co.uk - The Child Exploitation and Online Protection (CEOP) Centre has website which has been designed and written specifically for children of different ages to ensure children stay safe on the Internet. It also has sections specifically developed for parents/carers and teachers/trainers.

Online Safety Acceptable Use Agreement/Code of Conduct – Staff, Student Teachers and Governors

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Miss Brown. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Miss Brown.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.

I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

I will respect copyright and intellectual property rights, e.g. when using google image search only using results which have appropriate copyright.

I will not upload any materials about or reference to the school or its community on my personal social networks.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential. I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body.
- Personal or sensitive data taken off site must only be accessed on school hardware via the secure remote server.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under GDPR or for a Freedom of Information Request. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school; such a system would ensure as the user I was not saving files locally to my own device and breaching data security.

If I choose to wear a SmartWatch that contains the ability to take photos or recordings I will inform the Computing Lead, who will then be able to look into the features of the device to ensure it is acceptable within our school's AUP.

I will ensure that personal cameras or mobile phones will not be kept in teaching spaces.

Personal mobiles must never be used to access school emails and data. The only exception would publicised in exceptional circumstances with a clear time limit. In such situations, clear guidance for this purpose would be circulated by the Leadership Team.

Additional hardware/software

I will not install any hardware or software on school equipment without permission from the technical team.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSP or Deputy DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriateness of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues, I will secure, on every occasion, approval in advance for the material I plan to use with a member of the Senior Leadership Team.

Video conferencing

I will only use the conferencing tools that have been identified and risk-assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature ………………………………………………………………………………………… Date ……………………
Full Name …………………………………………….. (printed)
Job title ……………………………………………………………………………………

Wheatcroft Primary School

Pupil Acceptable Use Agreement /On Line Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- I understand my behavior in the virtual classroom should mirror that in the physical classroom.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Wheatcroft Primary School

Pupil Acceptable Use Agreement / Online Safety Rules

Dear Parent/ Carer

Computing including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Miller or Miss Brown, Wheatcroft School Online Safety Coordinators.

Please return the signed sections of this from which will be kept on record at the school.

-- ✂ --

Pupil Agreement

Pupil name…………………………………………………………………………….

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil Signature…………………………………………………………………………….

Parent(s)/Carer(s) Agreement

Parent(s)/Carer(s) Name …………………………………………………………………………….

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.)

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.
Parent(s)/carer(s) signature(s) ……………………………………………………

Date …………………………………………………………

Online Safety Acceptable Use Agreement/
Code of Conduct
Visitors, Coaches, Peripatetic Teachers and Supply Teachers

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all visitors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Miss Brown or the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Miss Brown, DSP or the Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. Schools may wish to add further constraints regarding contact with former pupils, e.g. giving consideration to ex-pupils who are also known to be 'vulnerable' young people up to the age of 25. Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSP, or a young person's or parent/carer's own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of a member of SLT.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP or Headteacher.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with a member of SLT.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature …………………………….…………… Date ……….………………
Full Name …………………………….. (Please use block capitals)
Job Title/Role ……………………………..………………………………

Online Safety Acceptable Use Agreement/Code of Conduct – Parent Helpers

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP or headteacher is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.

- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Signature …………………………………..………… Date ………………………

Full Name ………………………………….. (Please use block capitals)

Job Title/Role …………………………………..……………………………