Congerstone Primary School

Online Safety Policy

Status	Active
Sources	School Policy (KCISIE
Version	Sept 2022
Governors committee	All Governors- Pupil Outcomes
Consultation Period	Oct 22
Date approved	17th October 2022
Date of next review	Sept 2022 – (check alongside KCSIE updates)
Target group	Everyone – staff, children, governors and parents
Linked policies	Computing Policy Safeguarding Policy Photography Policy
Signed – Chair of Governors	
Signed – Headteacher	

Document History:

Version	Date of Review	Reviewed by:	Revisions made:
May 2022	Oct 2022	JA	Changes to ensure compatability with Sept 2022 KCSIE

Online Safety – Congerstone Primary School

Aims

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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Communicate regularly with parents to reinforce the importance of staying safe online.

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

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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

Roles and Responsibilities

The governing board

It is an expectation that governors hold Online Safety as a central theme in their whole setting approach to online safety. The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Safeguarding governor is Meeta Odedra. The governors receive Safeguarding training and the Safeguarding governor (and those wanting further training) will have additional Online Safety training based on the KCSIE 2022 updates.

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

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet – see appendices.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

- Governors should ensure that the school leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The DSL must uphold responsibilities outlined in KCSIE 2022 and must view online safety as a statutory part of the school's safeguarding responsibilities. In addition to this, when recruiting, the headteacher should consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/college might want to explore with applicants at interview.

The designated safeguarding leads

Details of the school's DSLs – Alison Ruff and Claire Simpson - are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager (Gavin King), Computing coordinator (Jodie Armstrong) and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged 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 board

This list is not intended to be exhaustive.

The ICT manager

Congerstone's ICT Manager is Gavin King, GSKS.

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. The current software that is used is provided by RM plc.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged 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

This list is not intended to be exhaustive.

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 (see appendices)
- Working with the DSLs (Alison Ruff and Claire Simpson) 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

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendix – age specific Acceptable Use agreements)

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

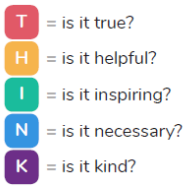
Visitors and members of the community

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

Managing the school **online** safety messages

We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

Online safety guidelines and the THINK rules will be prominently displayed around the school.



As a school, each year, we also participate in online safety activities during Safer Internet Day.

Every Wednesday the school will tweet the 'Wake-up Wednesday' message from National Online Safety (https://nationalonlinesafety.com/)

The parents regularly receive letters, emails, posters, and messages on homework sheets regarding online safety, internet, website and app guidance, and other updates regarding online safety.

All staff have the online safety training award accredited by National Online Safety (https://nationalonlinesafety.com/). The parents and governors have received several letters inviting them to partake in this training.

Online safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about online safety. Explicit teaching regarding Online Safety takes place mostly during, but not limited to, Computing sessions using Purple Mash, and during PSHE and Learning Means the World sessions. The following text is taken from the National Curriculum computing programmes of study and the guidance on relationships education, relationships and sex education (RSE) and health education.

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
- 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

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters, emails or other communications home, and in information via our website. Other useful resources may be shared via Twitter or Seesaw. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

Invitations to take part in Online Safety training in school may take place.

Invitations to take part in Online Safety provided by National Online Safety are sent out annually.

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.

Cyber-bullying

Definition

Child-on-child abuse is most often associated with cyber-bullying, though can include physical and sexual abuse, sexual harassment and violence, emotional abuse, teenage relationships abuse, emotional harm and grooming for sexual or criminal exploitation. 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.) We recognise that this can happen across age groups.

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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate, including additional emphasis during Safer Internet Day (Congerstone raises awareness for a week).

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/leaflets/tweets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSLs 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.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's online safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Managing the Internet
All internet activity within school is monitored and filtered through RM's SafetyNet system. If inappropriate use is detected, the ICT Manager is notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's digital devices.

If Internet research is set for homework, staff will remind students of their online safety training. Parents are encouraged to support and supervise any further research.

Infrastructure
Our internet access is provided by RM plc.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to the DSLs (Alison Ruff and Claire Simpson) teachers, Computing co-ordinator (Jodie Armstrong) or the IT technician (Gavin King).

Mobile Technologies
Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present, unless for the purposes of 2-factor authentication.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing email

The use of email within school is an essential means of communication for staff.

Pupils currently do not access personal email accounts within school, but where these accounts are provisioned, students are unable to email outside of the organisation.

Staff and governors must use the school's approved email system for any school business.

Staff must inform (the DSLs/ line manager/ IT technician) if they receive an offensive or inappropriate e-mail.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to act regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

Creation of videos and photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case, as they are all encrypted.

See also Photography Policy

Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, Twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on the school website, Twitter account, mobile app or any other school-based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops. These must be deleted after in line the guidelines set out in the General Data Protection Regulations 2018.

Misuse and Infringements

Complaints

Complaints or concerns relating to online safety should be made to the DSLs (Alison Ruff and Claire Simpson).

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the DSLs (Alison Ruff and Claire Simpson).

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by GSKS and then forwarded to the DSLs (Alison Ruff and Claire Simpson). Depending on the seriousness of the offence; investigation may be carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action, in accordance with aforementioned school policies and the Code of Conduct.

Equal Opportunities

Pupils with additional needs

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' online safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety.

Staff are given (or directed to) appropriate materials to teach online safety to all ages and abilities in a range of different formats. Typical examples include resources from CEOP, Safer Internet Day resources, Digiduck, etc.

Internet activities are planned and well-managed for children of all abilities and ages, and resources, work and support is differentiated appropriately.

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:
Department for Education (2021) https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes
Safer Internet Centre: http://www.saferinternet.org.uk/
UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis
CEOP - Think U Know - http://www.thinkuknow.co.uk/
National Online Safety: http://www.nationalonlinesafety.com
Childnet - http://www.childnet.com
Netsmartz http://www.netsmartz.org/index.aspx
Teach Today http://www.teachtoday.eu/
Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/
Byron Review ("Safer Children in a Digital World") http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/
Guidance for safer working practice for adults that work with children and young people
http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-andpractice/ig00311/
Information Commissioners Office/education: http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx
ICO guidance on use of photos in schools: http://www.ico.gov.uk/youth/sitecore/content/Home
Ofsted survey: http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-allby/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB
Plymouth Early Years E-Safety Toolkit: http://www.plymouth.gov.uk/early_years_toolkit.pdf
Protecting your personal information online:
http://www.ico.gov.uk/~/media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx

Getnetwise privacy guidance: http://privacy.getnetwise.org/

Children and Parents
National Online Safety: http://www.nationalonlinesafety.com
Vodafone Parents Guide: http://parents.vodafone.com/
NSPCC: http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internetsafety_wdh72864.html
Google guidance for parents: http://www.teachparentstech.org/
E-Parenting tutorials: http://media-awareness.ca/english/parents/internet/eparenting.cfm
Practical Participation – Tim Davies: http://www.practicalparticipation.co.uk/yes/
Digital Citizenship: http://www.digizen.org.uk/ Kent "Safer Practice with Technology":
http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-withtechnology-for-school-staff.aspx
Connect Safely Parents Guide to Facebook: http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html
Ofcom – Help your children to manage the media: http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/
Mobile broadband guidance: http://www.mobile-broadband.org.uk/guides/complete-resource-ofinternet-safety-for-kids/
Orange Parents Guide to the Internet: http://www.orange.co.uk/communicate/safety/10948.htm
O2 Parents Guide: http://www.o2.co.uk/parents FOSI – Family Online Internet Safety Contract: http://www.fosi.org/resources/257-fosi-safetycontract.html
Cybermentors (Beat Bullying): http://www.cybermentors.org.uk/
Teachernet Cyberbullying guidance: http://www.digizen.org/resources/cyberbullying/overview "Safe to Learn – embedding anti-bullying work in schools"
http://www.antibullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law,_policy_and_guidance/safe_to_l earn.aspx
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm Cyberbullying.org - http://www.cyberbullying.org/
CBBC – stay safe: http://www.bbc.co.uk/cbbc/help/home/

Technology
Kaspersky – advice on keeping children safe - http://www.kaspersky.co.uk/keeping_children_safe
Kaspersky - password advice: www.kaspersky.co.uk/passwords
CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/
Which Parental control guidance: http://www.which.co.uk/baby-and-child/child-safety-athome/guides/parental-control-software/
How to encrypt files: http://www.dummies.com/how-to/content/how-to-encrypt-important-files-orfolders-on-your-.html
Get safe on line – Beginners Guide - http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1
Childnet Parents and Teachers on downloading / music, film, TV and the internet - http://www.childnet.com/downloading/
Microsoft Family safety software: http://windows.microsoft.com/en-US/windows-vista/Protectingyour-kids-with-Family-Safety
Norton Online Family: https://onlinefamily.norton.com/
Forensic Software http://www.forensicsoftware.co.uk/education/clients.aspx

Legislation
To reiterate, this Policy is based on 'Keeping Children Safe in Education' 2015, last updated 2021.
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Overview of other related legislation:

Computer Misuse Act 1990
This Act makes it an offence to:
• Erase or amend data or programs without authority
• Obtain unauthorised access to a computer
• "Eavesdrop" on a computer
• Make unauthorised use of computer time or facilities
• Maliciously corrupt or erase data or programs
• Deny access to authorised users

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate
• Not kept longer than necessary
• Processed in accordance with the data subject's rights
• Secure
• Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
• Establish the facts
• Ascertain compliance with regulatory or self-regulatory practices or procedures
• Demonstrate standards, which are or ought to be achieved by persons using the system
• Investigate or detect unauthorised use of the communications system
• Prevent or detect crime or in the interests of national security
• Ensure the effective operation of the system.
• Monitoring but not recording is also permissible in order to:
• Ascertain whether the communication is business or personal
• Protect or support help line staff
• The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of

committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:
• The right to a fair trial
• The right to respect for private and family life, home and correspondence
• Freedom of thought, conscience and religion
• Freedom of expression
• Freedom of assembly
• Prohibition of discrimination
• The right to education These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Appendices: Please find the Acceptable Use agreements on the following pages.

CONGERSTONE PRIMARY SCHOOL

Acceptable Use Agreement

(For EYFS)

✓ I ask before I use a tablet, computer or camera.

✓ I tap or click on things I have been shown.

✓ I check if I can tap/click on things I haven't seen before.

✓ I tell a grown-up if something upsets me.

My Name: Class:

Parent/Carer Signed: Today's Date:

CONGERSTONE PRIMARY SCHOOL

KS1

Acceptable use agreement

I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.

I only open websites and activities that an adult has told or allowed me to use.

I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.

I keep my passwords safe and will never use someone else's.

I know personal information such as my address and birthday should never be shared online.

I know I must never communicate with strangers online.

I am always polite and presentable when I post to our communication tools, such as Seesaw, TEAMS, Email, etc.

I understand this agreement and know the consequences if I don't follow it.

My name: Class:
Parent/Carer signed: Today's date:

CONGERSTONE PRIMARY SCHOOL

KS2
Acceptable use agreement

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, email addresses, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as TT Rockstars, My Maths, Bug Club and Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as email, blogs and Seesaw carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I will ensure I am presentable when using live streaming services such as TEAMS/using recording devices such as cameras.
- Before I share, post or reply to anything online, I will T.H.I.N.K.

T = is it true?
H = is it helpful?
I = is it inspiring?
N = is it necessary?
K = is it kind?

- I will not use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, website etc.
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My name:	Class:	Parent/Carer signed:	Today's date:

CONGERSTONE PRIMARY SCHOOL

Parent and Carer Acceptable use agreement

Background and purpose Digital technologies are a powerful tool for learning providing access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate. It is therefore essential that children are fully equipped with the skills and knowledge to safely access and use digital technologies. Our **Parent/Carer Acceptable Use Agreement** is intended to help share the importance school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting. Our school aims to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks in school. Our school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, school expects children to demonstrate that they are responsible users of digital technologies at all times.	**Parents/Carers** We would ask parents and carers to support us by: ➢ Sharing good online behaviours with your child. ➢ Emphasising the importance of our Acceptable Use Statements/School's rules your child has agreed to. ➢ Highlighting the importance of accessing only age appropriate content and sites along with the pitfalls of social media. ➢ Explaining how to keep an appropriate digital footprint. ➢ Discussing what is and isn't appropriate to share online. ➢ Emphasising never to meet anyone online nor trust that everyone has good intentions. ➢ Reporting any concerns, you have, whether home or school-based. ➢ Stressing the importance of openness to discuss online experiences and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact. ➢ Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home. ➢ Follow our parental code of conduct and avoid posting or replying to any comments about our school on social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

Permission Access

By signing below, you

- agree to allowing your child access to the school's internet and ICT systems. This also includes any educational subscription services (including but not limited to TT Rockstars, My Maths, Bug Club, Seesaw, etc.)
- are also aware that your child has signed/agreed to the school's Acceptable Use Agreement for pupils.

Parent's/Carer's name: Signature: Date:

Child's name: Date:

Staff and Governor Acceptable use agreement

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times.

Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.

The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care in the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that permission has been granted by the headteacher in writing for each occurrence.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviours/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software using school devices unless permission has been given by the headteacher.
- I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
- I understand that mobile devices shall not be used, nor in my possession, during times of contact with children. These devices will be secured with adequate password protection on them should they be accessed by an unauthorised person.
- Any school trips/outings or activities that require a mobile phone/ camera will be provided by the school and any data collected on them will be used in accordance with school policies.
- At no point will I use my own devices for capturing images/ video or contact with parents/carers.

Staff name:	Signature:	Date: