Online Safety Policy

Policy

December 2023

Version 7

Sarah Abdulla ~ Headteacher

www.teaguesbridgeprimary.org

Written on:	December 2021
Reviewed on:	December 2023
Staff Responsibility	Mrs S. Abdulla/ M Hale
Governor responsibility	Stephen Reynolds

Safer Internet Policy

Rationale:

The use of technology is an integral part of our curriculum and provides children with the technological skills they will need to live in our modern World. At Teagues Bridge we use computing skills across all curriculum areas, this involves using internet to look at sources of information.

The internet provides pupils with unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisations and groups world-wide so as to increase skills, knowledge and abilities.

Our Ethos:

Teagues Bridge believes that the benefits to pupils accessing the resources of the Internet, far exceed the disadvantages. Ultimately, the responsibility for setting the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. Whilst we embrace technology we are not in favour of children using social- network sites such as Face book. We recognise that such sites are at the core of cyber-bullying and so we would strongly advise parents not to allow their children access and will inform parents and the local community support officers if we find these are being used in this way.

The purpose of this policy

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2020 and taken advise from other statutory documents: 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 cyberbullying 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. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures. This policy is a living

document and subject to full annual review but will also be amended where necessary during the year in response to developments in our school and the local area.

Online-safety risks are categorised as one of the 4 Cs: Content, Contact, Conduct or Contract. Many of the new risks are mentioned in KCSIE 2020, e.g. fake news and upskirting we keep updated with prominent new and emerging trends, through following safeblog.lgfl.net. There has been an alarming increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Contact and conduct of course also remain important challenges to address.

CORE	**Content** Child as recipient	**Contact** Child as participant	**Conduct** Child as actor	**Contract** Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

In past and potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some of your pupils may have missed opportunities to disclose such abuse during the first lockdown.

Aims:

This policy aims to:

- Set out expectations for all Teagues Bridge Primary school pupils and staff members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

• Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform

• Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online

• Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

o for the protection and benefit of the children in their care, and

o for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice

o for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (in-line with the school's Behaviour & Anti bullying policy)

Roles and responsibilities

All teachers and children have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher

Key responsibilities:

• Support safeguarding leads and technical staff as they review protections for pupils in the home and remote learning procedures, rules and safeguards

• Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding

• Oversee the activities of the DSL and ensure that their responsibilities listed are being followed and fully supported

• Ensure that policies and procedures are followed by all staff

• Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships

• Liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information

• Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the staff, DSL and governors to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data protection processes support careful and legal sharing of information

• Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles

• Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures

• Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

• Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised

• Ensure the school website meets statutory DfE requirements.

Designated Safeguarding Lead

Key responsibilities:

• "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety) … this lead responsibility should not be delegated." KCSIE 2023

• Work with the Headteacher and technical staff to review protections for pupils in the home and remote learning procedures, rules and safeguards

• Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." KCSIE 2023

• "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies." KCSIE 2023

• Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns

• Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply

• Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

• Work with the headteacher, SLT and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

• Stay up to date with the latest trends in online safety through receiving regular updates in online safety issues and legislation and be aware of local and school trends and undertake Prevent awareness training.

• Review and update this policy, other online safety documents and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.

• Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

• Ensure that online safety education is embedded across the curriculum and beyond, in wider school life

• Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents

• Liaise with school technical, pastoral, and support staff as appropriate

• Communicate regularly with SLT and the designated safeguarding governor to discuss current issues (anonymised), review incident logs and appropriate filtering and monitoring

• Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident

• Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

• Maintain up-to-date documentation of the school's online security and technical procedures

• Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown

• Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware

• Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying

Governing Body, led by Safeguarding Governor

Key responsibilities:

• Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges:

Questions from the Governing Board

• Ask about how the school has reviewed protections for pupils in the home (including when with online tutors) and remote-learning procedures, rules and safeguards

• "Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…" KCSIE 2023

• Support the school in encouraging parents and the wider community to become engaged in online safety activities

• Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings

• Work with the DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

• Check all school staff have read Part 1 and Annex A of KCSIE; check Annex C on Online Safety reflects practice in your school

• "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.

• "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". KCSIE 2023

• "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum

All staff

Key responsibilities:

• Recognise that RSHE will be introduced in this academic year and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject

• Understand that online safety is a core part of safeguarding; as such it is part of everyone's job

• Know who the Designated Safeguarding Lead (DSL) is and the Deputy DSLs are

• Read KCSIE 2023 and have a working knowledge of the document

• Read and follow this policy in conjunction with the school's main safeguarding policy

• Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.

• Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon

• Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

• Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites

• When supporting pupils remotely, be mindful of additional safeguarding considerations

• To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law

• Prepare and check all online source and resources before using within the classroom

• Encourage pupils to follow their acceptable use policy, at home as well as at school and remind them about it and enforce school procedures if not followed

• Notify the DSL of new trends and issues before they become a problem

• Take a zero-tolerance approach to bullying and low-level sexual harassment

• Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and violence) in the playground, corridors, toilets and other communal areas outside the classroom – always report to the DSL

• Receive regular updates from the DSL and have a healthy curiosity for online safety issues

• Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE Lead

Key responsibilities:

• Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives." KCSIE 2023

• This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

• Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.

Computing Lead

Key responsibilities:

• Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum

• Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

• Support the HT and DSL team as they review protections for pupils in the and remote-learning procedures, rules and safeguards

• Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

• Work closely with the DSL to ensure that school systems and networks reflect school policy

• Ensure all stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)

• Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and SLT with support from Telford and Wrekin ICT services

• Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

• With the support of the DSL, monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

• Maintain up-to-date documentation of the school's online security and technical procedures

Subject Area Leads

Key responsibilities:

• Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike

• Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context

• Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Volunteers and contractors

Key responsibilities:

• Read, understand, sign and adhere to an acceptable use policy Appendix D

• Report any concerns, no matter how small, to the DSL as named in the Acceptable Use Policies

• Maintain an awareness of current online safety issues and guidance

• Model safe, responsible and professional behaviours in their own use of technology at school and as part of

remote teaching or any online communications

Pupils

Key responsibilities:

• Read, understand, sign and adhere to the pupil acceptable use policy and review this annually Appendix A and B

• Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen

• Understand the importance of reporting abuse, misuse or access to inappropriate materials

• Know what action to take if they or someone they know feels worried or vulnerable when using online technology

• To understand the importance of adopting safe and responsible behaviours and good online safety practice

when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media

• Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher

• Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

• Read, sign and promote the school's Parental Home-School Contract and Parental Acceptable Use Policy.

• Consult with the school if they have any concerns about their children's and others' use of technology

• Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

• Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns

• Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible

• If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

External groups/ on site visitors

Key responsibilities:

• Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school and out of school when promoting the school

• Support the school in promoting online safety and data protection

• Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social

media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum

The following subjects have the clearest online safety links:

• PSHE including Relationships education and health education.

• Computing

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Teagues Bridge Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS including:

- Self-image & identity
- Online relationships
- Online reputation
- Copy right
- Ownership
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security

Handling online safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE. General concerns must be handled in the same way as any other safeguarding concern. School procedures for dealing with online-safety is detailed in the Child Protection & Safeguarding policy as well as the Behaviour & Anti-Bullying Policy. This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to DSL on the same day. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline. The school will actively seek support from other agencies, as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour, which we consider is particularly disturbing or breaks the law. For specific online safety concerns refer to the Child Protection and Safeguarding policy (Sexting, upskirting, bullying, sexual violence and harassment).Misuse of school technology (devices, systems, networks or platforms)Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks,connections, internet connectivity and devices, cloud platforms and social media

(both when on school site and outside of school). These are defined in the relevant Acceptable Use Policy as well as in this document. Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social Media incidents

We have clear rules and expectations of behaviour for children and adults when using social media in our school community. These are also governed by our school's Acceptable Use Policies the School's Online Communication Code of Conduct . Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Data protection and data security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

Rigorous controls on the Schools' network is set and maintained by Telford and Wrekin ICT services and the school monitors individuals usage using Senso. The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information. Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated who has the day-to-day responsibility of updating the content of the website. The site is managed by / hosted by Telford and Wrekin ICT services (School has its own gold technician. The DfE has determined information which must be available on a school website.

Where other staff submit information for the website,(IE news and class pages) they are asked to remember:

• School have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.

• Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose and for how long. Parents/carers answer as follows:

• For their child's photograph/video to be taken

• For displays around the school

• For social media

• For external use including: school website, paper-based school marketing and the newsletter

Class teachers have up-to-date lists of which children have permission to have photos or videos taken. These can be checked at any time on Bromcom. Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them). No

members of staff to use their personal phone to capture photos or videos of pupils and must be taken on school devise. Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy. Staff and parents are reminded annually (a signed declaration by parents with the Home- School Contract) about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

Staff, pupils' and parents Social Media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies, which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying,aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff)teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve). Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly dealswith issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on socialmedia platforms wherever possible and not encourage or condone underage use.However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, bringing the school into disrepute. We have an Online Communication (including Social Media) Code of Conduct for Staff Working with Children which all staff sign,

Social media incidents

Breaches of this policy and of school AUPs (Acceptable Use Policies) will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, we will request that the post be deleted and will expect this to be actioned promptly. Where an offending post has been made by a third party, the school may report it to the platform where it is hosted, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The police or other authorities may be involved where a post is potentially illegal or dangerous.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty (see Safeguarding Policy). Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature by the school. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Devise usage

All staff with access to school devices are reminded about rules on the misuse of school technology including when devices are used at home which should be used just like if they were in full view of a teacher or colleague. Personal devices including wearable technology and mobile telephone Pupils, who walk to or from school alone, are allowed to bring mobile phones in to school. Mobile phones have to be turned off before arrival on school property and not turned back on until the pupil has left the school premises. Upon arrival in the classroom, pupils should hand in their mobile phone to their class teacher who will keep them in an allocated space. During the school day, phones must remain turned off at all times and pupils should not attempt to access these.

At Teagues Bridge Primary all staff who work directly with children should leave their mobile phones on silent and only use them when they not teaching. Child/staff data should never be downloaded onto a private phone. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission should be sought from the site team or amember of SLT and this should be done in the presence of a member staff during school hours.

At Teagues Bridge Primary, parents are asked to be respectful when using their mobile phones on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

Network/internet access on school devices

Pupils are not allowed networked file access via personal devices.

Home devices are issued to some pupils. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked. The devices are filtered monitored when on home wifi connections.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours unless in an emergency. Staff can access the school Wifi but must understand that all internet traffic is monitored.

Volunteers, contractors, governors can access the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Parents have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be able to use their personal mobile phone in an emergency or in any other communication with the school. Support staff and volunteers should not be using their mobile phones at any other time unless authorised by the teacher leading the trip.In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains undesirable material, including but not exclusive to sexual images, violence or bullying.

Filtering and Monitoring

What is filtering and monitoring?

- Filtering – Effectivity Filtering Systems block students from harmful content, denying access to any harmful content.
- Monitoring – Monitoring systems monitor the on-screen activity of students. Reporting what websites Students are on, the content of the website, and what the students are typing online and offline in search bars, word documents, and chat messages.

Role of SLT

- Filtering – Effectivity Filtering Systems block students from harmful content, denying access to any harmful content.
- Monitoring – Monitoring systems monitor the on-screen activity of students. Reporting what websites Students are on, the content of the website, and what the students are typing online and offline in search bars, word documents, and chat messages.

Role of DSL

- Work closely with IT service providers to meet the needs of your setting.
- Take a lead responsibility for safeguarding and online safety, which could include overseeing and acting on:
- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

Role of ICT provider

- Work closely with IT service providers to meet the needs of your setting.
- Take a lead responsibility for safeguarding and online safety, which could include overseeing and acting on:
- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

Role of teachers

- Work closely with IT service providers to meet the needs of your setting.
- Take a lead responsibility for safeguarding and online safety, which could include overseeing and acting on:
- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

Pupil Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, e-mails and other digital devices.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username or password.
- I will be aware of 'Stranger Danger', when I am communicating on-line.
- I will not disclose personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or message or anything that makes me feel uncomfortable when I see it on-line.
- I will not enter chat rooms/blog sites without adult permission.

I understand that everyone has equal rights to use technology as a resource and:

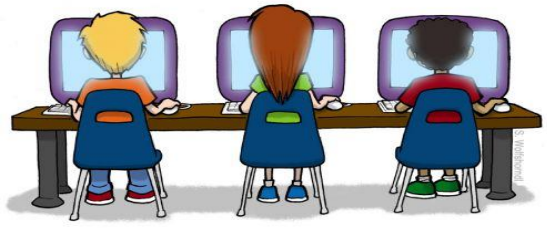
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT system for on-line gaming or video broadcasting (you Tube), unless I have permission from a teacher.
- I will not print work from the internet unless I have permission from a teacher.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or alter any other files, without the owner's knowledge or permission.
- I will be polite and responsible when I communicate with others, I will never use inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain security and integrity of technology it offers me and to ensure the smooth running of the school:

- I will only use personal hand held devices in school if I have permission. I understand that, if I do use my own device in school, I will follow the rules set out in this agreement.
- I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filter/security systems in place.
- I will immediately report any damages or faults involving equipment or software, however this may have happened.
- I will not open attachments to e-mails unless I know and trust the person who sent the e-mail.
- I will not install or attempt to install programmes or alter computer settings.
- I will only use social network sites with permission from the teacher/Parent.



When using the internet for research, I recognise that:

- I should ensure that I have permission to use the original work.
- Where work is protected by copyright, I will not download copies.

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents that are not acceptable and are outlined in this agreement. This includes when I am outside of school e.g. cyber bullying, use of images or sharing personal information).
- I understand that if I fail to comply with the Acceptable Use Policy Agreement, I will be subject to specific actions set out by the headteacher. This may include loss of access to the school network, behaviour plan, parents will be contacted and in the event of illegal activities, police will be involved.

Think then CLICK

These rules help us to stay safe on the Internet

- We only use the internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can write polite and friendly emails to people that we know.

Think then CLICK

These rules help us to stay safe on the Internet. We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they choose to use.

- We ask permission before using the Internet.
- We only use websites approved by an adult.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately turn off the screen if we not sure about a website.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We do not download anything.
- We ask before printing anything out.

Please complete the sections below to show you have read, understood and agree to the rules included in the agreement. If you do not sign and return this agreement, access will not be granted to the school ICT systems.

Teagues Bridge Primary School
Responsible E-mail and Internet use

Please complete, sign and return to your teacher as soon as possible

Pupil:	Base:

Pupils agreement (to be signed by the pupil)

- I have read and understood the school E-mail and Internet Use Policy Agreement.
- I will use the computer system and internet in a responsible way and follow the rules at all times

Signed:	Date:

Parents/Carers Consent for Internet Access

- I have read and understood the school E-mail and Internet Use Policy Agreement and give permission for my son/daughter to access the internet.
- I have understood that the school will take responsible precautions to ensure pupils cannot access appropriate materials.
- I understand that the school cannot be held responsible for the nature or content of material accessed through the internet.
- I agree that the school is not liable for any damages arising from the use of the internet facilities.
- I give permission for my child to take part in videoing as part of their curriculum work.

Signed:	Date:

Please print name:

Parent/Carer's Consent for Web Publication of Work and Photographs

- I agree, that if selected, my son/daughter's work may be published on the school Website.
- I also agree that photographs and videos that include my son/daughter may be published subject to the schools rules that full names will not be used.
- As parents, we will support the school's approach to e-safety and will not upload or add any pictures, video or text that could potentially upset, offend or threaten the safety of any member of the school community (e.g. uploading a photograph of a school Christmas concert with names on a Facebook page). No reference to Teagues Bridge Primary School should be made on social network sites (this includes all members of the school community).

Signed:	Date:

On occasions other media organisations may come into school and interview the children for publication in order to promote the school and celebrate in your child's achievements (e.g. local newspaper or radio shows). Local newspapers will often include a picture of your child and print their names. If you are happy for your child to take part in media activities of this nature please sign below.

Signed: _____ Date: _____