EASTINGTON PRIMARY SCHOOL

Online Safety Policy
and
Acceptable Use Agreement

September 2024
(To be reviewed September 2026 or before if needed)

To be read in conjunction with: Behaviour, Anti-Bullying, Safeguarding, Safer Working Practice, Social Media, Code of Conduct & Whistle Blowing policies, Eastington Primary School Filtering and Monitoring Policy

THE RATIONAL

Online safety encompasses internet technologies and electronic communications such as iPads, smart TVs and wireless technology. The internet is a powerful resource which can enhance and potentially transform learning and teaching when used effectively and appropriately. This policy highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy aims to:

● Set out expectations for all Eastington Primary School community 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 and young people 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 and young people 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 (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

FURTHER HELP AND SUPPORT

Internal school channels should always be followed first for reporting and support, as documented in school policies. Safeguarding concerns and incidents should be reported in line with our Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and typically the headteacher will handle referrals to the LA designated officer (LADO). Our local authority may also advise/offer general support.

EDUCTION AND CURRICULUM

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Computing
- PSHE and Relationships education, relationships and sex education (RSE)

It is the role of all staff to follow the planned curriculum to support online safety/safeguarding as well as looking for other opportunities to reinforce online safety. Staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RSE).

Whenever overseeing the use of technology (devices, the internet etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff carefully supervise and guide pupils in learning activities involving online technology (including, extra-curricular, 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.

ROLES AND RESPONSIBILITIES

This school is a community and all members 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.

KEY RESPONSIBILITIES FOR STAFF:

- Recognise that online safety and computing teaching is a whole-school subject requiring the support of all staff; online safety has become core to this subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will deal with an issue
- Know who the Designated Safeguarding Lead (DSL): Catrin Parsons and Deputy Safeguarding Leads: Zoe Avastu, Rachel Carrick and Jemma Redpath.
- Read Part 1, Annex B of Keeping Children Safe in Education
- 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.
- Understand that online safety/safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/computing lead if policy does not reflect practice in your school
- Follow the school planning, in PHSE, RSE and computing, which has a strong focus on online safety. In addition, make the most of learning opportunities when they arise.
- Whenever overseeing the use of technology in school or for homework, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- Carefully supervise or guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright.
- Be aware of security best-practice at all times, including password hygiene

● Prepare and check all online sources and resources before using
● Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school rules on site.
● Notify the DSL/computing lead of new trends and issues before they become a problem
● Discuss bullying and low-level sexual harassment with your DSL and action will be taken in line with the anti-bullying and safeguarding policy. Record on CPOMS.
● Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/computing lead know
● Receive regular updates from the DSL/computing lead and have a healthy curiosity for online safeguarding issues
● Model safe, responsible and professional behaviours in their own use of technology.

KEY RESPONSIBILTIES FOR PUPILS:

- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually

● 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, including any concerns about any adult
● Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
● To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school.
● 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

KEY RESPONSIBILITIES OF PARENTS OR CARERS:

- Read, sign and promote the school's parental acceptable use policy when their child joins the school.

● 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
● If they have any concerns about their children's and others' use of technology, please contact the school if you think we or other agencies would be able to support you.

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/RSE).

General concerns must be handled in the same way as any other safeguarding concern; all stakeholders should talk to the computing lead / designated safeguarding lead so these concerns can be logged to highlight a potential problem.

Any online safety issues and incidents will be managed in line with the school child protection policy. Online safety incidents are logged and dealt with appropriately in line with the filtering and monitoring policy.

The online world develops and changes quickly. New opportunities, challenges and risks are appearing all the time. The DSL supported by the DSL team and computing lead will stay up to date with the latest devices, platforms, apps, trends and related threats. The school has strong links with local police including the local BEAT officer, who supports staff and children with this.

The school will help pupils recognise acceptable and unacceptable behaviours by:
● looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
● looking at how online emotions can be intensified
● teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and considering unacceptable online behaviours often passed off as so-called social norms or just banter.

The school will help pupils identify and manage risk by:
● discussing the ways in which someone may put themselves at risk online,
● discussing risks posed by another person's online behaviour,
● discussing when risk taking can be positive and negative,
● discussing "online reputation" and the positive and negative aspects of an online digital footprint.

This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example,
● discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
● asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

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.

SEXTING

We refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools.) NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.)

There is a one-page overview called Sexting; how to respond to an incident - see below - which we follow as it is important that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

Sexting: how to respond to an incident

An overview for all teaching and non-teaching staff in schools and colleges

UK COUNCIL FOR **CHILD INTERNET SAFETY**

This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'.

All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line with your school's safeguarding policies.

The DSL should be familiar with the full 2016 guidance from the UK Council for Child Internet Safety (UKCCIS), ***Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People***, and should **not** refer to this document instead of the full guidance.

What is 'sexting'?

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as **the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18**. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'.

'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

What to do if an incident involving 'sexting' comes to your attention

Report it to your Designated Safeguarding Lead (DSL) immediately.

- **Never** view, download or share the imagery yourself, or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- **Do not** share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

If a 'sexting' incident comes to your attention, report it to your DSL. Your school's safeguarding policies should outline codes of practice to be followed.

For further information

Download the full guidance Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016) at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.

The school DSL will in turn use the school safeguard policy. The DSL may use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved (see link: https://www.icmec.org/wp-content/uploads/2017/02/Sexting-in-Schools-UKCCIS.pdf). We will always seek further advice form other agencies, if needed.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

UPSKIRTING

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education. In our school children are not allowed phones/watches with photo capacity – if these are needed they will be handed in to the class teacher in the morning and returned to the child at the end of the day.

BULLYING – See Anti-Bullying Policy

Online bullying in school will treated like any other form of bullying, the school Anti-Bullying Policy will be followed and incidents logged on CPOMS. This can sometimes referred to as cyberbullying, could include issues arising from online banter.

SEXUAL VIOLENCE AND HARASSMENT

Guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours viewed by some as 'low level' are treated seriously and not allowed to perpetuate.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow safeguarding procedures.

MISUSE OF SCHOOL TECHNOLOGY (DEVICES, SYSTEMS, NETWORKS AND PLATFORMS)

Clear and well communicated rules and procedures are essential to ensure positive pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media. These are expanded on in the relevant Acceptable Use Agreements as well as in this document. We reinforce these expectations/rules at the beginning of any school year as the Acceptable Use agreement is shared with children.

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 conduct policy.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology.

SOCIAL MEDIA INCIDENTS

Breaches will be dealt with in line with the school behaviour policy (for pupils) or Conduct Policy (for staff).

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre – 0344 381 4772 https://swgfl.org.uk/services/professionals-online-safety-helpline/?gclid=EAIaIQobChMIoNmpuKSN8wIVRofVCh3lewRIEAAYASAAEgJsjPD_BwE) for support or help to accelerate this process.

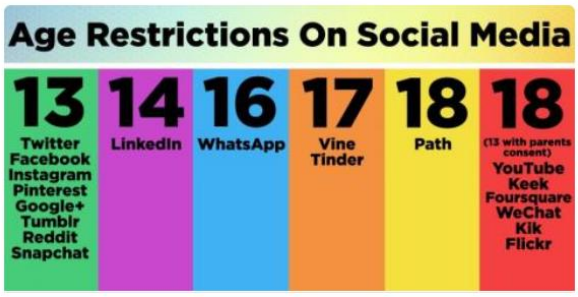
SOCIAL MEDIA PRESENCE OF STAFF, PARENTS AND PUPILS – See Social Media Policy

Social media (including 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. As stated in the Social Media Policy, Safer Working Practice Policy, Acceptable Use policy/agreement and conduct Policy, which all members of the school community are included in, 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.

If parents have a concern about the school, we want and expect them to contact us directly and in private to hear & resolve the matter effectively. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and other parents, undermine staff morale and the reputation of the school (which is important for the pupils and families we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). We recognise these age restrictions have been put in place to support the safeguarding and well-being of children and support parents adhering to these age restrictions.



The school has to strike a difficult balance of not encouraging underage use at the same time as well as preparing children for future use of these platforms. 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. We have strong links with the BEAT Officer who leads active, interactive sessions with Y6 on Online Safety to augment our curriculum too.

Children will often learn most from the models of behaviour they see and experience, which will often be from adults at school and at home. Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive learning at school the next day). School can sign post parents to useful and supportive websites if parents have concerns to support parent/child discussion about online safety. These are regularly sent home via the newsletter and letters.

Email is the official electronic communication channel between parents and the school. 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; if any requests are made, staff will reject or ignore them.
Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). We accept that cannot control this (but this highlights the need for staff to remain professional in their private lives/parents to monitor their children's online use).
Staff must not follow such pupils accounts.
Where pre-existing family links between a family/staff member, these should be declared/approved with the headteacher upon entry of the pupil or staff member to the school.

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 avoid inappropriate sharing and oversharing online and have the strictest privacy settings. They should never discuss the school, the staff or its stakeholders on social media and they should be careful their personal opinions might not be attributed to the school or local authority, bringing the school into disrepute.

DATA PROTECTION AND DATA SECURITY

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies). All relevant information can be shared without

consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.
From 'Data protection: a toolkit for schools'

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. The use of Egress email to send confidential safeguarding information internally or externally.

To support data protection and security we:

- Use on the SWGfL network, which has rigorous controls and filtering
- Have two-factor authentication for staff to access emails and online storage.
- Use encrypted email (Egress) for sensitive/safeguard information
- Only school emails are used for school information
- Password protect laptops and hard drive devices
- Bitlocker is turned on so laptops are encrypted
- Backed up teacher information to online and hard drive storage (Admin has separate back-up regime in line with GCC)
- Grant wireless access to school devices only
- Regularly update anti-virus software (IT technician)
- School laptops are not left unattended in cars etc.

APPROPRIATE FILTERING AND MONITORING – see Filtering and monitoring policy.

At this school, the internet connection is provided by SWGfL. This means we have a dedicated and secure connection that is protected.

At Eastington Primary School, we have decided that the below options most appropriate because they will ensure that pupils can only access websites available through the school network (subject to filters set up) with the additional monitoring provided by adults in the classroom throughout any online activities.

There are two types of appropriate monitoring used in school:
1. Physical monitoring (adult supervision in the classroom)
2. Internet and web access provided by: SWGfL

The ICT technician makes monthly checks on the filtering system and produces and shares a report with the DSL and Headteacher. Filtering and monitoring procedures for the school are reviewed annually.

ELECTRONIC COMMUNICATIONS

EMAIL

Staff use school emails (not personal) for communication with parents. Log in to staff e-mails/cloud storage requires two-factor authentication system. School emails can be accessed by school admin if needed.

General principles for email use are as follows:

- School e-mail is the only means of electronic communication to be used between teachers/admin and parents (in both directions). TAs do not communicate with parents through e-mail – any such e-mails will go through the SENCo/class teacher/admin.

- School e-mail is to be used for admin-teachers/teachers-teacher, teacher-TA to communicate.
- Email may only be sent using the school email system. There should be no circumstances where a private email is used to discuss children or any sensitive matter; if this happens by mistake, the DSL/Headteacher (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- If sensitive data needs to be shared between staff (ie. Safeguarding issues), Egress systems are used.
- Appropriate behaviour is expected at all times - the system should not be used to send inappropriate materials or use language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff

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. SLT/admin have the day-to-day responsibility of updating the content of the website.

Where other staff submit information for the website, they will:

- Credit sources and use material only with permission.
- Pupil images and videos can be published on the website, with parental consent, however pupils names will not be used so they can be identified unless we have parent permission.
- Where pupil work published on the website only first names are used.

(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 (beyond internal assessment, which does not require express consent). Parents answer as follows:

- They do not wish for photos/recordings of their child to be taken at all
- They allow photos/recordings to be used for displays around the school
- They allow photos/recordings to be shared outside of school
- They allow photos/recordings to be shared outside of school with first name (from Sept 2022)

We adhere to parents wishes, though we acknowledge that in large events/trips with members of the public it can sometimes be difficult to prevent images being taken.

Whenever a photo or video recording is taken/made in school, the member of staff taking it will check the latest parent consent before using it for any purpose.

At Eastington Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils. Each class has a school camera and ipdad and these will be used. Images/recordings will be stored on school equipment/cloud storage only and deleted when no longer needed.

All staff are governed by their contract of employment, the Safer Working Practice Policy, Social Media Policy, the Online Safety Policy, Acceptable Use Agreement and the school's Conduct Policy which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.

Staff and parents are reminded regularly about the importance of not sharing photos of other members of the school community without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We ask all parents not to post photos of staff or other children on social media without seeking permission from all those in the photo.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are advised to be very careful about placing any personal photos on social media outside school. They are taught to understand the need to maintain privacy settings so as not to make public, personal information. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images, that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

DEVICE USAGE

PERSONAL DEVICES INCLUDING MOBILE PHONES & WEARABLE TECHNOLOGY

- Pupils are not allowed to bring mobile phones/wearable technology to school. If needed in an exceptional circumstance the phone will be handed into the office/classteacher, where it will be looked after and handed to the child at the end of the day. Important messages and phone calls to or from parents can be made at the school office. The office will also pass on messages from parents to pupils in emergencies.

● All staff who work directly with children should leave their mobile phones/wearable technology on silent and only use them in private staff areas during school hours.

- Staff should put phones away not have them with them when moving around school if children are on site (including before and after school childcare). In an emergency/exceptional circumstance where breaking this guidance may be necessary, this should be discussed with the HT.
- If staff use their mobile phone to access emails/calendar, they must log out after and never use an unsecure or public network connection.

● Volunteers, contractors, governors should leave their phones on silent. 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 of the headteacher should be sought (the headteacher may choose to delegate/supervise this).
● Parents are asked put phones away when they are on site. They should not take any photos, on site unless given permission.

NETWORK / INTERNET ACCESS ON SCHOOL DEVICES

● Pupils are allowed to access the school wireless internet network for school-related internet use within the framework of the acceptable use policy.
● Outside school staff 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 are permitted to use their personal mobile phone for emergency use or to call the school if necessary. Teachers using their personal phone in an emergency to contact a parent will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.
Staff are not to use mobile phones to take photos and instead, they will use a school camera or iPad.
On trips, occasionally, staff phone numbers will need to be shard with parent helpers. Staff must be explicit in explaining the number is only to be used on that day for that trip.

APPENDIX 1

ACCEPTABLE USE AGREEMENT FOR STAFF:

WHAT IS AN ACCEPTABLE USE AGREEMENT?
We ask all children, young people and adults involved in the life of Eastington Primary School to sign an Acceptable Use Agreement, which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
This is reviewed annually, and staff will be asked to sign it upon entry to the school and every time changes are made.

WHY DO WE NEED AN ACCEPTABLE USE AGREEMENT?
All staff and governors, have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

WHERE CAN I FIND OUT MORE?
All staff and governors should read Eastington Primary School's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, Anti-Bullying & Harassment Policy, Safer Working Practice Policy, Code of Conduct Policy & Whistle Blowing Policy, etc).

If you have any questions about this acceptable use agreement or our approach to online safety, please speak to SLT or the computing leader.

ACCEPTABLE USE POLICY FOR STAFF, GOVERNORS AND VOLUNTEERS

WHAT AM I AGREEING TO?

1. I have read and understood Eastington Primary School's full Online Safety policy/Social Media Policy/Code of Conduct Policy/Safer Working Practice Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils.

2. I understand it is my duty to support a whole-school online safety safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead.

3. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the computing, PHSE/RSE curriculum.

4. Any use of devices in school will be protected by filtering systems and security measures/systems through antivirus software. When using devices at home, school devices are protected through security measures/systems using antivirus software.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by
・not sharing other's images or details without permission
・refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same, to the headteacher.

7. I will follow the online safety policy for digital images and videos as well as social media.

8. I understand the importance of upholding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either.

9. I agree to adhere to all provisions relating to data protection within the school online safety policy, whether or not I am on site or using a school device, platform or network. I will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the headteacher/computing lead/IT technician if I suspect a breach. I will only use complex passwords (eg: not something easily identifiable such as a pet name/date of birth etc) which include capital letter/number/special character and not use the same password as for other systems.

10. I will not store school-related child/adult information, data, photographs on personal devices, storage or cloud platforms. Back up hard drives will provided by school and belong to school. They will be encrypted/password protected. I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

11. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to

bypass security or monitoring and will look after devices loaned to me.

12. I understand and support the commitments made in the Online Safety Policy & Acceptable Use Agreement and will report any infringements in line with school procedures.

13. I will follow the guidance in the Safeguarding, Online-Safety, Social Media policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I will follow the guidance in the sections on handing incidents and concerns about a child in general and relating to sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

14. I understand that breach of this agreement and/or of the school's full Online Safety Policy/Social Media Policy may lead to staff disciplinary action or termination of my relationship with the school and where appropriate, referral to authorities such as the police.

15. I will follow the guidance regarding the use of mobile phones in school. I will not take photos or videos on my mobile or use my mobile phone around children.

To be completed by the user:

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

APPENDIX 2

ACCEPTABLE USE AGREEMENT FOR KS2

KS2 Pupil Acceptable Use Agreement

I understand that I must use school technology in a responsible way, to ensure that there is no risk to my safety or to the safety of others.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school computers/iPads are primarily intended for learning.
- 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 act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any one else's files.
- I will be polite and kind when I communicate with others.
- I will not take or distribute images or photos of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and look after the school technology:

- I understand the risks and will not try to access any materials which I have not been asked to do so.
- I will report any damage to school equipment however this may have happened.
- I will not open any links unless I know and trust them.
- I will not install programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful.

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 if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school but involve my membership of the school community (examples would be online-bullying, use of images or sharing personal information/images of others without permission).
- I understand that if I break this acceptable use agreement, I may lose access to the school network/internet, or my parents/carers may be contacted.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- 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, using learning websites that I log into (e.g. Times Table rockstars).

Name: _____ Signature: _____

Class: _____ Date: _____

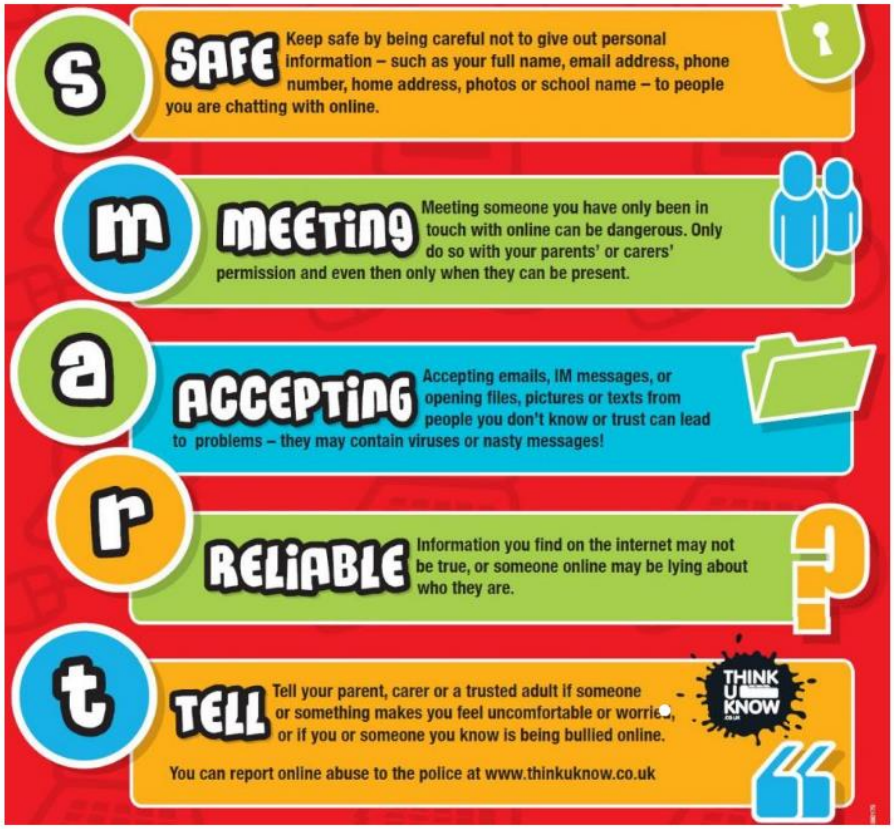
APPENDIX 3

ACCEPTABLE USE AGREEMENT FOR KS1

KS1 Online Safety and Acceptable Use Agreement

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet
- I will also follow the SMART rules we discussed in class.



My name: _____ Signature: _____ Class: ____

APPENDIX 4

ACCEPTABLE USE AGREEMENT FOR RECEPTION

Eastington Primary School

Acceptable Use Agreement for Reception

If I am unhappy I tell someone

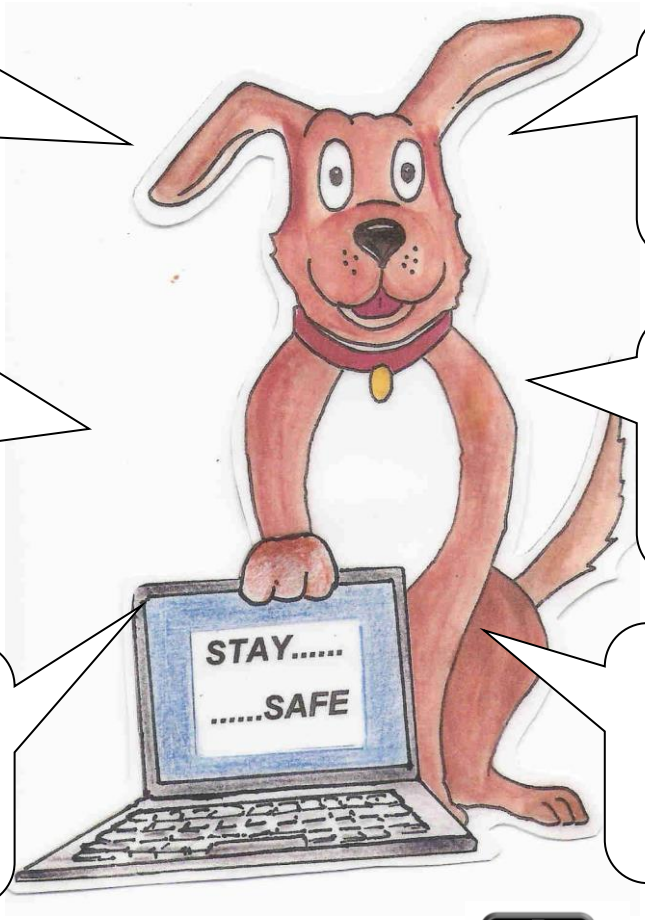
I am kind and polite to others online

I don't talk to people I don't know

I am careful with my password

I won't use pictures that I'm not allowed to

I know not to believe everything I read



My name

Class *Class _____*

I agree ☺

Date

APPENDIX 5

Below are items related remote learning, which are no longer relevant.

From main policy:

Key responsibility of parents of carers:

● Support the child during remote learning to ensure video lessons occur in a neutral place with suitable backgrounds (ie. not in a bedroom, with the camera pointing away from personal information or with other members of the household in the background etc.). Please ensure children and adults in view are fully dressed.

Network/ Internet access of school devices

● Laptops (e.g. for vulnerable students) are issued to some children in lockdowns to support home learning. These laptops have been prepared by the IT Technician for use (updated virus/software/work of other children deleted etc). An agreement is signed by parents who borrow this equipment - these laptops are restricted to the apps/software installed by the school and may be used by the child for learning only and not for personal use.

From KS1 acceptable use policy:

- If I am learning at home (during remote learning), I will follow these rules. I will also ensure I act as I do in school during live lessons (ie. Put up my hand and use kind words). I will make sure I am dressed (not in pyjamas) and ready to learn.

From KS2 acceptable use policy:

For my own personal safety:

- During remote learning and live lessons, I will keep my identity private (ie. my background will be neutral and appropriate). I will also ensure I am dressed appropriately and not in pyjamas

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

- During remote learning and live lessons, I will act as I do in school. (raise hand to answer questions, not chat or use emojis and not take photos or videos of the lesson)

I recognise that the school has a responsibility to maintain the security and look after the school technology:

- I will not record any live lessons during remote learning.

From staff, governors and volunteers acceptable use policy:

3. During remote learning:

o I will not behave any differently towards students compared to when I am in school. I will never attempt to arrange any meeting, without the full prior knowledge and approval of the headteacher, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

o I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.

o I will conduct any video lessons in a professional environment as if I am in school (not a public or personal space). This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable. The camera view will not include any personal information or inappropriate objects.

- o I will record live lessons. This is for my protection as well as that of pupils.
- o I will not take secret recordings or screenshots of myself or pupils during live lessons.