



# **ONLINE SAFETY POLICY**

# Contents

Overview .....	2
Aims .....	2
Further Help and Support .....	2
Scope .....	2
Roles and responsibilities.....	3
Headteacher – Norma Hewins .....	3
Designated Safeguarding Lead– Shaun Acharya .....	4
Governing Body, Safeguarding Link Governor – Ally Rae.....	5
All Jubilee Primary School staff.....	6
Jubilee Primary School PSHE / RSE Lead – Josh Cardale/ Sheilla Patel .....	7
Computing Lead – Josh Cardale.....	7
Subject / aspect leaders .....	<a href="#">87</a>
ICT Technician – Emilio Fuentes.....	8
LGfL TRUSTnet Nominated contacts – Norma Hewins and Emilio Fuentes.....	<a href="#">98</a>
Volunteers.....	9
Pupils.....	9
Parents/carers.....	<a href="#">109</a>
Appendix A: Acceptable Use Policy for Parents and Carers.....	10
Appendix B: Acceptable Use Policy for Key Stage 1 Pupils.....	12
Appendix C: Acceptable Use Policy for Key Stage 2 Pupils.....	13

## Overview

### Aims

This policy aims to:

- Set out expectations for online behaviour, attitudes and activities and use of digital technology (including when devices are offline)- at Jubilee Primary School.
- 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:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - 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 Safeguarding and Child Protection Policy, 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 policy documents, especially in response to incidents, which should be reported in line with the Safeguarding and Child Protection Policy. The DSL will handle referrals to Local Authority Multi-Agency Safeguarding Hubs (MASH) and the Headteacher will handle referrals to the LA Designated Officer (LADO).

### Scope

This policy applies to all members of the Jubilee Primary School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school or centre role.

## Roles and responsibilities

All members of the school community have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare children for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school.

### Headteacher – ~~Norma Hewins~~ Josh Cardale

#### Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the Designated Safeguarding Lead (DSL) and ensure that the DSL responsibilities listed in the section below 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 DPO, 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
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident including sexual violence, sexual harassment while making reference to section 27 in the Safeguarding and Child Protection Policy (Further Information on Safeguarding Issues).
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- 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 the school website meets statutory requirements

## Designated Safeguarding Lead– Shaun Acharya

### Key responsibilities

All quotes below are from Keeping Children Safe in Education September 2024<sup>42</sup>:

- “It is essential that children are safeguarded from potentially harmful and inappropriate online material.”
- “The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”
- Ensure that “All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.
- An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate.”
- “Liaise with the local authority and work with other agencies in line with Working Together to safeguard children”
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headteacher, DPO 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
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for Behaviour, Safeguarding and Child Protection, Prevent and others) and submit for review to the governors.
- Receive regular updates in online safety issues and legislation. Ensure that online safety education is embedded across the curriculum through RHSE and with the support of outside agencies.
- 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 (Senior Leadership Team) and the designated safeguarding governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how 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
- Oversee and discuss 'appropriate filtering and monitoring' with governors
- Ensure the ~~DfE Guidance on Sexual violence and Sexual Harassment- (2021)~~~~is~~~~2021~~ is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying making key references to section 27 in the Safeguarding and Child Protection Policy (Further Information on Safeguarding Issues).
- Facilitate training and advice for all staff:
  - all staff must read KCSIE Part 1 and all those working with children Annex A
  - it would also be advisable for all staff to be aware of Annex C (online safety)
  - cascade knowledge of risks and opportunities throughout the organisation including to wider stakeholders i.e. parents and governors.
- Ensure the school is meeting the Digital and Technology Standards in accordance with the most up-to-date DfE regulations.
- Ensure the school pastoral team are proactively supporting pupils stay safe online.
- Signpost websites (like below) that support parents to safeguarding and protect their children stay safe on the internet or devices at home:
  - <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
  - <https://saferinternet.org.uk/guide-and-resource/parents-and-carers>
  - <https://www.bark.us/tech-guide/app-management-spotify/>

## **Governing Body, Safeguarding Link Governor – Ally Rae-Nicole Edwards**

### **Key responsibilities (quotes are taken from Keeping Children Safe in Education 2021):**

- 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](#)
- “Ensure an appropriate **senior member** of staff, from the school or college 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...”
- 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 DPO, 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 I of KCSIE; SLT and all working directly with children have read Annex A; check that 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. The training should be regularly updated [...] in line with advice from the local three safeguarding partners [...] integrated, aligned and considered as part of the overarching safeguarding approach.”
- “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”.
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...]

## All Jubilee Primary School staff

### Key responsibilities:

- 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 pick it up
- Know who the Designated Safeguarding Lead (DSL) is.
- Read Part I, Annex A and Annex C of Keeping Children Safe in Education (whilst Part I is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the Jubilee main Safeguarding and Child Protection Policy with key emphasis placed on section 27 (Further Information on Safeguarding Issues)
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with safeguarding procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the Jubilee Primary School staff Acceptable Use Policy and Code of Conduct/handbook
- 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, 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/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)

- 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/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the ~~DSL~~ **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 sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues.  
They must 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.

## Jubilee Primary School PSHE / RSHE Lead –Sheilla Patel

### Responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships, Health and Sex 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.”
- Make reference to Section 27 of the Safeguarding and Child Protection Policy (Further Information on Safeguarding Issues- Online Safety).
- 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 / RSE.

## Computing Lead – Emily Bland

### Key responsibilities:

- As listed in the ‘all staff’ section, plus:



- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum and Safeguarding and Child Protection Policy.
- Work closely with the DSL/ and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- 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.

## Subject / aspect leaders

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in their 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
- Ensure subject specific action plans also have an online-safety element

## ICT Technician – Emilio Fuentes

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- 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. Make specific reference to section 27 in the Safeguarding and Child Protection Policy (Further Information on Safeguarding Issues- Filters and monitoring).
- Work closely with the Designated Safeguarding Lead / Data Protection Officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above 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 senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- 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

- Monitor the use of school technology and online platforms and that any misuse/attempted misuse is identified and reported in line with school policy

## LGfL TRUSTnet Nominated contacts – ~~Norma Hewins~~ Josh Cardale and Emilio Fuentes

### Key responsibilities:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at [gdpr.lgfl.net](https://gdpr.lgfl.net)

## Volunteers

### Key responsibilities:

- Read, understand, sign and adhere to the Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the DSL
- Maintain an awareness of current online safety issues and guidance in reference to the Safeguarding and Child Protection Policy.
- Model safe, responsible and professional behaviours in their own use of technology

## Pupils

### Key responsibilities:

- Read, understand, sign and adhere to the student/pupil Acceptable Use Policy and review this annually
- 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
- 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 Acceptable Use Policy (AUP) and read the pupil AUP and encourage their children to follow it
- 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.

### Related Jubilee Primary School Policies include:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Social Media Policy
- Data Protection Policy
- Data Breach Policy
- Acceptable Use Policies (see appendices)

<https://www.jubilee.hackney.sch.uk/about-us/school-information/school-policies/>

## Appendix A: Acceptable Use Policy for Parents and Carers



### Acceptable Use Policy (AUP) for PARENTS AND CARERS

#### What is an AUP?

We ask all children, young people and adults involved in the life of Jubilee Primary School to sign an Acceptable Use Policy (AUP), which is a document that 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). Your child will also be asked to sign an AUP as part of the Computing curriculum.

#### Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

**“Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”**

#### Where can I find out more?

You can read Jubilee’s full Online Safety Policy [here](#) for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc.). If you have any questions about this AUP or our approach to online safety, please speak to a member of the senior leadership team.

#### What am I agreeing to?

1. I understand that Jubilee Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my 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.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent [LGfL DigiSafe](#) survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
9. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: [childrenscommissioner.gov.uk/our-work/digital/5-a-day/](https://childrenscommissioner.gov.uk/our-work/digital/5-a-day/)
10. I understand and support the commitments made by my child in the pupil Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules (AUPs for each key stage are available to read on the school website.)
11. I can find out more about online safety at Jubilee Primary School by reading the full Online Safety Policy [here](#) and can talk to my child's class teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

## Appendix B: Acceptable Use Policy for KS1 pupils



### Acceptable Use Policy (AUP) for KS1 PUPILS

My name is \_\_\_\_\_

To stay **SAFE online and on my devices**:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone

✓

My trusted adults are:

\_\_\_\_\_ at school

\_\_\_\_\_ at home

## Appendix C: Acceptable Use Policy for KS2 pupils



### Acceptable Use Policy (AUP) for KS2 PUPILS

#### **This agreement will help keep me safe and help me to be fair to others**

1. *I learn online* – I use the school’s internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. *I ask permission* – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. *I am creative online* – I don’t just spend time on apps, sites and games looking at things from other people. I get creative and learn to program and present using computer software.
4. *I am a friend online* – I won’t share anything that I know another person wouldn’t want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. *I am a secure online learner* – I keep my passwords to myself and reset them if anyone finds them out. Friends don’t share passwords!
6. *I am careful what I click on* – I don’t click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. *I ask for help if I am scared or worried* – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. *I know it’s not my fault if I see or someone sends me something bad* – I won’t get in trouble, but I mustn’t share it. Instead, I will tell a trusted adult. If I make a mistake, I don’t try to hide it but ask for help.
9. *I communicate and collaborate online* – with people I already know and have met in real life or that a trusted adult knows about.
10. *I know new online friends might not be who they say they are* – I am careful when someone wants to be my friend. Unless I have met them face to face, I can’t be sure who they are.
11. *I check with an adult before I meet an online friend* face to face for the first time, and I never go alone.
12. *I don’t do live videos (livestreams) on my own* – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. *I keep my body to myself online* – I never get changed or show what’s under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don’t send any photos or videos without checking with a trusted adult.



14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

~~~~~

**I have read and understood this agreement.**

**If I have any questions, I will speak to a trusted adult: at school that includes my teacher and other members of staff.**

**Outside school, my trusted adults are** \_\_\_\_\_

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_