

Sacred Heart  
Catholic Primary School



Learning in Love

## **SOCIAL MEDIA POLICY 2024-26**

### Mission Statement

Guided by truth, respect and compassion; we share in building upon every individual's foundation, nurturing a love of learning in preparation for tomorrow's society, with Jesus at the heart of all we do.

Governing Body with Responsibility	Ethos and Admissions Committee
Agreed by Governors on	22.5.24
Chair's Signature	
Staff Member Responsible for Review	Headteacher
Date for Review	May 2026

## **Contents**

1. Aims
2. Legislation and Guidance
3. Roles and responsibilities
4. Rationale

## **AIMS**

1. To create for all children a secure, happy and caring environment conducive to their educational, emotional and social development, fostering self-control and consideration for others, and promoting self-esteem.
2. To help pupils broaden their experience and knowledge of the immediate environment and wider world and to understand the interdependence of individuals, groups and nations. 3. To help pupils develop lively, enquiring minds, the ability to question and argue rationally, to apply themselves to tasks, to solve problems and make choices and judgements.
4. To help pupils use language, ICT and mathematics effectively.
5. To identify and cater for children with special needs.
6. To develop respect for religious and moral values and tolerance of other races and religions.
7. To provide for all children equal opportunities for the development of their creative instincts and physical skills and to encourage an aesthetic awareness.

## **Legislation and guidance**

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's guidance on [protecting children from radicalisation](#).

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

The policy also takes into account the [National Curriculum computing programmes of study](#).

## **Definitions**

Definitions of social media are detailed in appendix I

## **Roles and responsibilities**

### **The Governing Body**

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

### **The Headteacher**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The headteacher will

- address any online safety issues or incidents
- Ensure that any online safety incidents are logged (on MyConcern safeguarding software and/or behaviour logs) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged (on MyConcern safeguarding software and/or behaviour logs) and dealt with appropriately in line with the anti-bullying policy
- Update staff on online safety as part of the safeguarding CPD plan
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the Governing Body

This list is not intended to be exhaustive.

### **All staff, student teachers and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 4 & 5)
- Working with the Designated Safeguarding Lead to ensure that any online safety incidents are logged (MyConcern safeguarding software and/or behaviour logs) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the anti-bullying policy

Members of staff, student teachers and volunteers must not be a member of any social media group which is created to discuss or share information about the school.

This list is not intended to be exhaustive.

All Staff, student teachers and volunteers will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

## **Parents**

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 4 & 5)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>

Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>

Parent and Carer Toolkit factsheet, Childnet International: <https://www.childnet.com/resources/parent-and-carer-toolkit/>

All parents will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

## **Pupils**

The school's Acceptable Use Policy (AUP) makes it clear to pupils what use of social media is allowed. This states that, 'Social network sites should never be accessed/used within school'.

Pupils must not be a member of any social media group which is created to discuss or share information about the school.

All pupils will

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4 & 5)

## **Visitors and members of the community**

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

## **Rationale**

At Sacred Heart Catholic Primary School, the governors and staff fully recognise the contribution the school makes to safeguarding children. We recognise that the safety and protection of all pupils is of paramount importance and that all staff, including volunteers, have a full and active part to play in protecting pupils from harm. We believe that the school should provide a caring, positive, safe and stimulating environment which promotes all pupils' social, physical, emotional and moral development.

Sacred Heart Catholic Primary School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

- Encouraging the responsible use of social media in support of the Sacred Heart Catholic Primary School's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our pupils from cyber bullying.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.

Ultimately, effective safeguarding of children can only be achieved by putting children at the centre of the system, and by every individual and agency playing their full part, working together to meet the needs of our most vulnerable children, in line with Keeping Children Safe in Education.

### **Training of Staff**

At Sacred Heart Catholic Primary School, we recognise that early intervention can protect pupils who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at risk pupils.

### **Use of social media sites by employees in a personal capacity**

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner. Staff will be advised as follows:

- That they familiarise themselves with social network sites' privacy settings in order to ensure that information is not automatically shared with a wider audience than intended. It is recommended that, as a minimum, all privacy settings are set to 'friends only', irrespective of use/purpose.
- That they must not conduct or portray themselves, or allow friends to portray them, in a manner which may:
  - Bring the school into disrepute;
  - Post pictures or videos that lead to valid parental complaints;

- Be deemed as derogatory towards the school and/or its employees;
- Be deemed as derogatory towards pupils, parents/carers or governors
- Bring into question their appropriateness to work with children
- Contravene current National Teacher Standards
- That they should not form online friendships or enter into communication with parents/carers as this could lead to professional relationships being compromised.
- That they must not form online friendships or enter into online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised.
- That they must not post pictures or negative comments about the school, pupils, parents or colleagues including Governors or school events.
- That they must never disclose sensitive, private or confidential information across private messaging.
- That they consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion, which could result in their professional reputation being compromised.
- That they consider what they 'like', 'share' or 'follow' on social media sites e.g. politics and religion, which could result in their professional reputation being compromised.
- That if their use of social media/networking sites contravenes this policy, they may be subject to disciplinary action.

Inappropriate use by employees should be referred to the Head teacher in the first instance.

### **Creation of social media accounts by school staff for use in education**

All social media services must be approved by the Headteacher in advance of any educational work being undertaken.

### **Comments posted by parents/carers on social media sites**

- Parents/carers will be made aware of their responsibilities regarding their use of social media via this policy (in particular when their child joins the school), the school website, letter and school newsletters.
- Parents/carers must not post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents of other children pictured.
- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media.
- Parents/carers must not post malicious or fictitious comments on social media sites about the school or any member of the school community.

- Parents must not form online friendships or enter into online communication with members of staff as this could lead to professional relationships being compromised.

The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step, the school will discuss the matter with the parent to try and resolve the matter and to ask that the relevant information be removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the School considers inappropriate, the School will consider taking the following action: -

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this;
- Set out the school's concerns to you in writing, giving the parent/carer a warning and requesting that the material in question is removed;
- Contact the police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed; or in cases where the posting has a racial element, is considered to be grossly obscene or is threatening violence;
- If the inappropriate comments have been made on a school website or online forum, the school may take action to block or restrict that individual's access to that website or forum;
- Contact the host/provider of the Social Networking site to complain about the content of the site and ask for removal of the information;
- Take other legal action against the individual.

### **Parent/carer usage of WhatsApp groups**

WhatsApp/social media groups are not an official school channel of communication but at Sacred Heart, we recognise that social media is a useful tool for class representatives and parents.

- Out of respect for other children and their families, parents/carers must not discuss individual children on WhatsApp/social media groups.
- Parents/carers are advised to contact school should they have any concerns regarding their child and should not use this platform to discuss other children or incidents that are being managed within school.
- Misinformation (or information that is inappropriate) being shared by members of the school community does cause unnecessary distress to children as well as parents/carers and staff.
- School requests that any comments shared on social media be kept factual and supportive, with links to the official school information where possible.
- Parents/carers with concerns that these rules (designed to support all families) are not being followed should take 'screenshots' and contact school for support.
- We ask that any communication remains professional and respectful for all within our community.
- Any parent/carer should not share individual phone numbers with others without that consent as this would be a GDPR breach.

All class reps and parents in class groups report any breaches to school immediately so that communication and respect for all members of our community remain professional, respectful and

supports our collective community. Breaches of these rules, including communication of inaccurate information, is deeply upsetting to members of our school community.

### **Dealing with incidents of online (cyber) bullying**

The schools Anti Bullying Policy makes sanctions regarding bullying using new technologies very clear. Page 5 of DfE's 'Behaviour and Discipline in Schools' indicates that the school can take action against incidents that happen outside of school if it:

- Could have repercussions for the orderly running of the school
- Poses a threat to another pupil or member of the public
- Could adversely affect the reputation of the school

Use of social networking sites to harass, bully or intimidate pupils would be covered by this irrespective of when/where the post was made.

### **Be SMART Online**

At Sacred Heart Catholic Primary School, we encourage pupils to take a SMART approach to social media behaviour:

**Safe** – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.

**Meeting** – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.

**Accepting** – We advise that pupils only accept emails and other forms of communication from people they already know.

**Reliable** – We teach pupils about the dangers of believing everything they see online.

**Tell** – We encourage pupils to tell a teacher, parent or carer if they see or read anything online that makes them feel uncomfortable.

### **Safeguarding of Children**

Children have their photographs taken to provide evidence of their achievements for their development records. Staff, visitors, volunteers and pupils are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day.

In accordance with Merton Safeguarding Children Board Document – 'Harmful Sexual Behaviour Protocol, June 2017, we will:-

- Where there is a concern that a child has displayed or committed problematic or harmful sexual behaviour, a consultation will be taken with MASH (Multi-Agency Safeguarding Hub).
- Where there is a concern that a child may have been a victim of harmful sexual behaviour, a referral will be made to the police.

Appendix I - Definitions

**Sacred Heart Catholic Primary School defines** “social media” as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:

- Blogs
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media sharing services
- ‘Micro-blogging’ applications, such as Twitter; Snapchat
- Mobile TV applications such as Sky Sports

Social Media sites such as ‘Twitter’ and ‘Facebook’ state that children should be 13 years of age to use them (this was initially developed from American law). In the UK the minimum age for ‘WhatsApp’ is 16. Therefore, no primary age children should be using or accessing these types of social media sites

**Sacred Heart Catholic Primary School defines** “cyber bullying” as any use of social media or communication technology to bully an individual or group.

**Sacred Heart Catholic Primary School defines** “members of the school community” as any teacher, member of support staff, pupil, parent/carer of pupil, governor or ex-pupil. The internet provides a range of social media tools that allow users to interact with one another, for example: from rediscovering friends on social networking sites such as Facebook to keeping up with other people’s lives on Twitter and maintaining pages on internet encyclopaedias such as Wikipedia. Whilst recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Sacred Heart Catholic Primary School staff and contractors are expected to follow when using social media. This policy applies to

- personal webspace such as social networking sites (for example Facebook, Instagram),
- blogs
- microblogs such as Twitter,
- chatrooms or messaging sites such as WhatsApp and Messenger,
- forums,
- podcasts,
- open access online encyclopaedias such as Wikipedia,
- social bookmarking sites such as del.icio.us
- content sharing sites such as TikTok, Instagram and YouTube.

The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium. The policy is based around 5 key areas

- The use of social networking sites by pupils within school.
- Use of social networking by staff in a personal capacity.
- Creation of network accounts by staff for use in education.
- Comments posted by parents/carers.
- Dealing with incidents of online bullying.

<b>Acceptable Use Agreement: All Staff, Volunteers and Governors</b>
--

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any Local Authority (LA) system I have access to.
- I will ensure all documents, data etc, are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.  
This is currently: LGfL StaffMail
- I will only use the approved email system and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the head teacher.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones/devices at school and only use in staff areas.

- I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites/tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the LGfL system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the Designated Safeguarding Lead (DSL) if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the DSL.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- *Staff that have a teaching role only:* I will embed the school's on-line safety/digital literacy/ counter extremism curriculum into my teaching.

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature

Date

Full Name (printed)

Job title / Role

**Authorised Signature (Head Teacher / Deputy)**

I approve this user to be set-up on the school systems relevant to their role

Signature Date

Full Name (printed)

▪ **Acceptable Use Policy for Parents/Carers**

**Internet and ICT:** As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. I understand that the school can, if necessary, check my child's computer files and the internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

**Use of digital images, photography and video:** I understand the school has a clear policy on the use of digital images and video and I support this. I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities. I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose. I will not take and then share online, photographs or videos of other children (or staff) at school events without permission.

**Social networking and media sites:** I understand that the school has a clear policy on the use of social networking and media sites and I support this. I will raise queries, concerns or complaints directly with the school rather than posting them on social media. I will not post malicious or fictitious comments on social media sites about the school or about any member of the school community. I will not form online friendships or enter into online communication with members of staff as this could lead to professional relationships being compromised. I understand that social media sites have minimum ages and I will follow these.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

**My daughter / son name(s):** \_\_\_\_\_

**Parent / carer signature:** \_\_\_\_\_

**Parent/ carer name:** \_\_\_\_\_

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

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

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

My trusted adults are:

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

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

## KS2 Pupil Acceptable Use Agreement

- 
- These statements can keep me and others safe & happy at school and home
- 1. ***I learn online*** – I use the school’s internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored.
- 2. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when 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 to learn and make things.
- 4. ***I am a friend online*** – I won’t share or say anything that I know would upset another person or they wouldn’t want shared. If a friend is worried or needs help, I 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 app add-ons can cost money, so it is important I always check.
- 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 a parent/carer before I meet an online friend*** 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 when using a device with 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 someone 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 follow age rules*** – 13+ games aren't good for me so I don't use them. Games may be scary, violent or unsuitable. 18+ games are very unsuitable. Social network sites have a minimum age of at least 13 and should never be accessed/used within school.
17. ***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.
18. ***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).
19. ***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, at home and at school.
20. ***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.
21. ***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 and/or report it.
22. ***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.
23. ***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. If I am not sure I ask a trusted adult.
24. ***I learn even when I can't go to school (eg because of Covid-19)*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the

classroom and nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.

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

**If I have any questions, I will speak to a trusted adult.**

My trusted adults are:

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

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

**My Name:** \_\_\_\_\_

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

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