PUDSEY BOLTON ROYD
PRIMARY SCHOOL

'We enjoy. We achieve.'

Care Growth Teamwork

Online Safety Policy

Date of ratification: **Nov 2025**

Ratified by: **Governing Board Committee**

Date of review: **Nov 2027 or sooner if needed**

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its safe use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

3. Legislation and Guidance

This policy is based on the Department for Education's (DFE's) statutory safeguarding guidance, Keeping Children Safe in Education (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on:

- Teaching Online Safety in Schools (https://www.gov.uk/government/publications/teaching-online-safety-in-schools)
- Preventing and Tackling Bullying (https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and Cyber-Bullying: Advice for Headteachers and School Staff (https://www.gov.uk/government/publications/preventing-and-tackling-bullying)
- Relationships and Sex Education (https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education)
- Searching, Screening and Confiscation (https://www.gov.uk/government/publications/searching-screening-and-confiscation)

It also refers to the DFE's guidance on Protecting Children from Radicalisation (https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the Education Act 1996 (https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the Education and Inspections Act 2006 (https://www.legislation.gov.uk/ukpga/2006/40/contents) and the Equality Act 2010 (https://www.legislation.gov.uk/ukpga/2010/15/contents).

In addition, it reflects the Education Act 2011 (http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), 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.

4. Roles and Responsibilities

4.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will co-ordinate meetings with appropriate staff to discuss online safety and monitor online safety by liaising with a member of the safeguarding team. There is a nominated governor who oversees online safety. All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's Information & Communication Technology (ICT) systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with Special Educational Needs & Disabilities (SEND) because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- They should review the standards of filtering and monitoring and discuss with IT staff and service providers what more needs to be done to support school in meeting the expected government standard.
- Governing bodies should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

4.2 The Headteacher

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

4.3 The Designated Safeguarding Team

Details of School's Designated Safeguarding Leads (DSLs) are set out in our Safeguarding and Child Protection Policy (SCPP), as well as relevant job descriptions. These are displayed around school and available for all visitors to the school to see as they sign into the building and parents can see who they are on the 'Safeguarding' page of School's website.

The Designated Safeguarding Team takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working alongside the Headteacher, Computing Team and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with School's SCPP
- Ensuring that any relevant online safety incidents are logged on the Child Protection Online Monitoring System (CPOMS) in line with the School's SCPP
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School's Behaviour Policy
- Appropriately responding to incidents involving the sharing of nude or semi-nudes. (https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)
- Updating and delivering staff training on online safety
- Endeavouring to keep parents/carers up to date with current concerns or threats through messages using the School Ping and/or Safer Schools apps, linking to online advice and support
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board.

This list is not intended to be exhaustive.

4.4 The Computing Team

The Computing Team is responsible for working alongside the Senior Leadership Team (SLT) and other outside providers to:

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at School, including terrorist and extremist material. Harmful and inappropriate content without unreasonably impacting teaching and learning.
- Ensure that users are effectively and reliably prevented from generating or accessing harmful and inappropriate content

- That any generative AI product used must maintain robust activity logging procedures. This function may be integrated into an AI tool or be provided by an additional solution working on top of an AI product. That input prompts and responses are monitored
- Ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with School's Behaviour Policy.

This list is not intended to be exhaustive.

4.5 All Staff and Volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix C), and ensuring that pupils follow the school's terms on acceptable use (Appendix A and Appendix B)
- Working with the DSL team to ensure that any online safety incidents are logged in accordance with the school's safeguarding procedures, currently using the CPOMS system, and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

4.6 Parents/Carers

Parents/Carers 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 A and Appendix B)
- 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 resource sheet – Childnet International (https://www.childnet.com/resources/parents-and-carers-resource-sheet)
- Healthy relationships – Disrespect Nobody (https://www.disrespectnobody.co.uk/).

4.7 Visitors and Members of the Community

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

5. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum: In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- That abuse may occur from other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages and sharing of inappropriate images.
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- That they need to challenge what they see online, that through the use of AI and other technologies they maybe exposed to computer generated images and information that are not a true reflection on reality.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Educating Parents/Carers about Online Safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via our website, e-mails or through meetings and events to help educate and inform parents. This policy will also be shared with parents/carers via the School website.

School will share information with parents/carers as necessary to keep them informed of new and potentially harmful popular trends and direct them to online resources to give them appropriate information on how to keep their child safe. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's class teacher. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

7. Cyber-Bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see also School's Behaviour Policy.)

7.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class – online safety discussions are built into the medium-term plans for Computing curriculum lessons.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber- bullying. This includes Personal, Social, Health and Economic education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL team will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7.3 Examining Electronic Devices

School staff have specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm;
- And/or disrupt teaching;
- And/or break any of the School rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the SLT to decide whether they should:

- Delete that material;
- Or retain it as evidence (of a criminal offence or a breach of School discipline);
- And/or report it to the police*

  ** Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.*

Any searching of pupils will be carried out in line with:

- The DFE's latest guidance on Screening, Searching and Confiscation (https://www.gov.uk/government/publications/searching-screening-and-confiscation)

- United Kingdom Council for Child Internet Safety guidance on Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People (https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through School's Complaints Policy.

8. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices A-D). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. Designated staff will act upon instant notifications generated by the system. More information is set out in the acceptable use agreements in Appendices A, B, C and D.

8.1 Pupils using Mobile Devices in School

Pupils are not to bring mobile phones into School without the express consent of a senior leader. On the rare occasions that this permission is granted, and parents/carers have signed the appropriate paperwork, the phone will be handed to the class teacher on arrival at the School site in the morning, for it to be locked away and returned only once the child is leaving School at the end of the day. If a mobile phone is brought into School without permission, on the first occasion it will be returned to the parent/carer by the teacher. On subsequent occasions the parent/carer will have to make an appointment with a senior leader for the phone to be returned in order for a discussion to be had around seeking to prevent further occurrences.

8.2 Staff using Personal Equipment in School

Where school staff have brought their own personal equipment (such as mobile telephones, digital assistants, laptops and cameras into the school), these personal items should not be used or available during pupil contact sessions unless authorised by either the Headteacher or Deputy Headteacher.

Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role and must not be connected to School networks without express permission. Such equipment should be locked away in a cupboard or filing cabinet and only taken out

at suitable times in the day if needed, such as lunch times, when children are not present in the room. Personal devices should never be used to capture, record or share images of children or events related to school unless express permission from the Headteacher has been granted. In these circumstances, the member of staff must ensure that the images/videos are copied onto a School device and the images removed from their personal device as soon as possible.

8.3 Staff using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software or asking an appropriate member of School staff to do this for them
- Keeping operating systems up to date – always install the latest updates or ask an appropriate member of staff for assistance in doing this.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix D. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from a member of the Computing Team.

9. Staff use of Social Media

School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security and privacy settings available through social networking sites and ensure that they keep them updated as the sites change their settings, as well being aware of who may be linking to their account. Staff are advised that inappropriate communications that come to the attention of School, can lead to disciplinary action, including dismissal.

10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems, the internet or a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSLs will undertake child protection and safeguarding training which will include online safety at least every 2 years. They will also update their knowledge and skill base on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our SCPP.

12. Monitoring Arrangements

Alerts generated will be investigated and actions taken as deemed necessary following School's Behaviour Policy. School will have systems in place to track and monitor the use of the internet in school and will put systems in place to identify the individual who has generated the alert. Class based staff will need to ensure that children log on with their individual details and do not sure these to ensure the effectiveness of the monitoring system.

A DSL will log behaviour and safeguarding issues related to online safety using the CPOMS system if it relates to a child, or in personnel folders if it relates to inappropriate conduct by a member of staff.

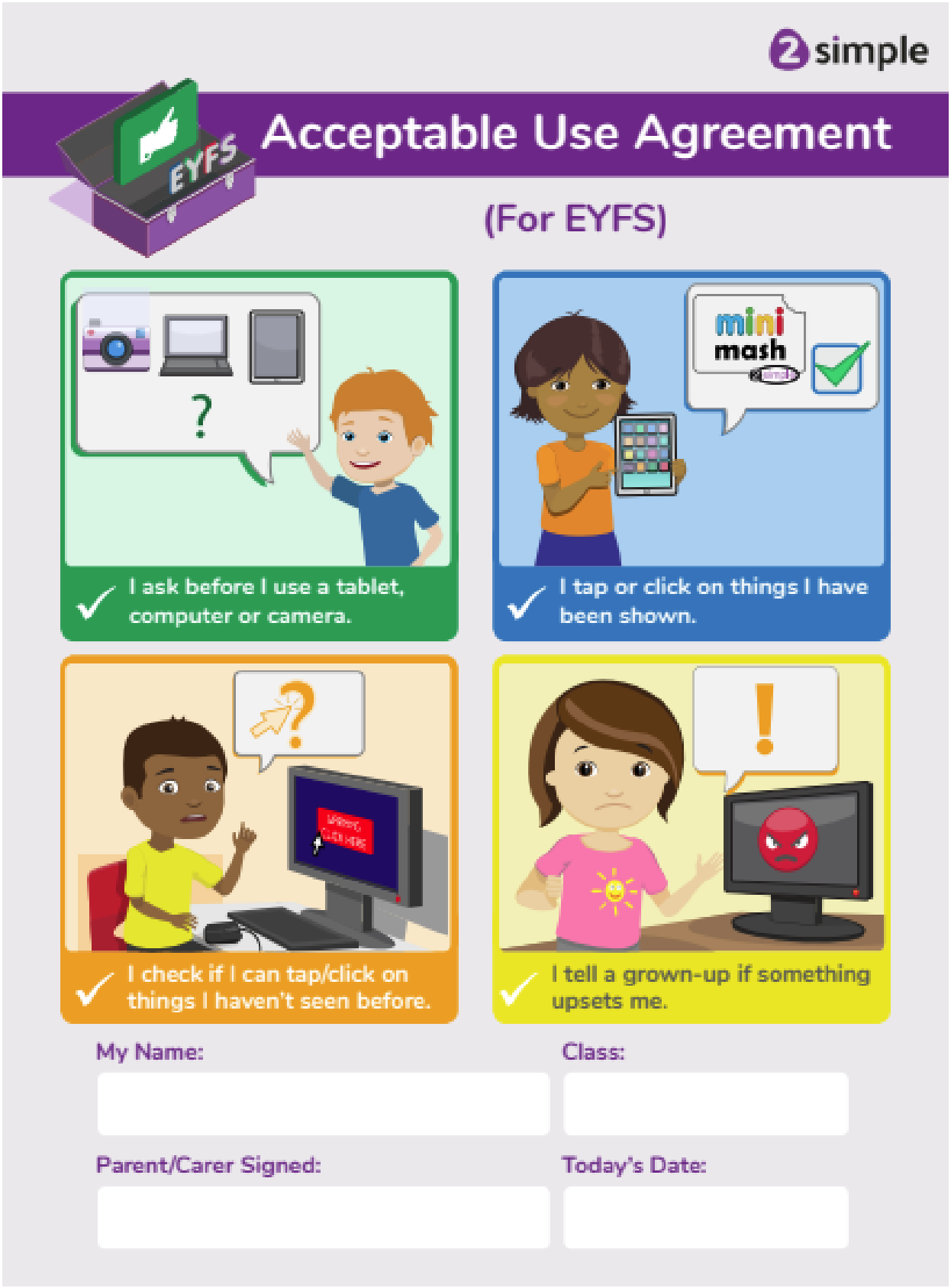
This policy will be reviewed biannually, or as required, to consider and reflect the risks pupils face online, this is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Mobile Phone Policy
- Behaviour Policy
- Disciplinary Policy
- Complaints Procedures
- Acceptable internet use procedures

ONLINE SAFETY POLICY APPENDIX A: EYFS Acceptable Use Agreement



ONLINE SAFETY POLICY APPENDIX B: KS1 Acceptable Use Agreement

Acceptable Use Agreement

- ✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ✓ I only open activities that an adult has told or allowed me to use.
- ✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ✓ I keep my passwords safe and will never use someone else's.
- ✓ I know personal information such as my address and birthday should never be shared online.
- ✓ I know I must never communicate with strangers online.
- ✓ I am always polite when I post to our blogs, use our email and other communication tools.

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

My Name:	Class:
Parent/Carer Signed:	**Today's Date:**

ONLINE SAFETY POLICY APPENDIX B: KS2 Acceptable Use Agreement

Acceptable Use Agreement

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

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

- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

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

My Name: Class:

Parent/Carer Signed: Today's Date:

ONLINE SAFETY POLICY APPENDIX B: Staff Acceptable Use Agreement

2simple

Acceptable Use Agreement

(Staff)

Background and purpose

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

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

The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

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

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care about the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that permission has been granted by the headteacher in writing for each occurrence.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.
- I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.

Staff Name: **Signature:** **Date:**