



Singleton Church of England Primary School

Online Safety Policy



“Passion for learningPassion for life”

Vision

“With God all things are possible” Matthew 19:26

“I have come so that they may have life and have it to the full” John 10:10

To provide the children with a variety of challenging and enriching opportunities, enabling them to live life to the full. Developing a growth mind-set, believing that with God everything is possible. To show, love , trust, wisdom and respect, becoming exemplary role models in our community and the wider world.

School lead for this policy:	Kate James
Committee with oversight for this policy -	Governance Committee
Policy to be approved by the Governance Committee	Autumn 2023
Policy / Document due for review	Autumn 24
Ratified at the Governance Meeting	
Chair:	Alec Davies

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school	8
8. Pupils using mobile devices in school	8
9. Staff using work devices outside school	8
10. Learner Passwords	8
11. How the school will respond to issues of misuse	9
12. Training	9
13. Monitoring arrangements	10
14. Links with other policies	10
15. Filtering and monitoring	
Appendix 1: EYFS and KS1 acceptable use agreement	10
Appendix 2: KS2 acceptable use agreement	12
Appendix 3: Parent/carers acceptable use agreement	Error! Bookmark not defined.
Appendix 4: Staff/governors/visitors acceptable use agreement	17
Appendix 5: Community users acceptable use agreement	20
Appendix 6: Example online safety incident report log	22
Appendix 7: Responding to incidents of misuse	23

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 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

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, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- › **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- › [Relationships and sex education](#)
- › [Searching, screening and confiscation](#)

It also refers to the DfE'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.

3. Roles and responsibilities

3.1 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 regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Simon Willcock.

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 4)
- › Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- › 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 and/or disabilities (SEND). This is 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

3.2 The Computing Subject Leader

The computing subject leader is Kate James. She is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

In addition, she must;

- › 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.
- › Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- › Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- › Ensure that any online safety incidents are logged (see appendix 6) and dealt with appropriately (see appendix 7)
- › Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

At Singleton School, we subscribe to Lancashire ICT, who support our computing subject leader to ensure all of the above is in place. Lancs ICT come to school on a monthly basis, however they can be contacted at any time for help and support.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL and computing subject leader take responsibility for online safety in school, in particular:

- › Supporting each other in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with other staff, as necessary, to address any online safety issues or incidents
- › Managing all online safety issues and incidents in line with the school child protection policy
- › Ensuring that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy
- › Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- › Updating and delivering staff training on online safety
- › 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 – these reports will be checked on a monthly basis and signed by the schools SHE committee. The reports are kept in the main office.

3.4 All staff 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 ICT systems (appendix 4), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- › Working with the DSL to ensure that any online safety incidents are logged (see appendix 6) 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'

3.5 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 (appendices 1 and 2)
- › Agreeing and adhering to the terms on acceptable use of the school's ICT systems (appendix 3),

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

- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet International](#)
- › Parent resource sheet – [Childnet International](#)

3.6 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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 5).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

At Singleton Primary School we following planning from Purple Mash and Education for a connected World,

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
- › 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

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.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters and emails home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during class workshops. All parents are invited to their child's class workshop, where an element of online safety will be covered at the beginning of the session.

The school will let parents know:

- › What systems the school uses to filter and monitor online use
- › What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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.

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 (PSHE) 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 (see section 12 for more detail).

The school also sends information/leaflets on cyber-bullying to parents 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 will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and](#)

[confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

- › The DfE's latest guidance on [searching, screening and confiscation](#)
- › UKCIS guidance on [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 the school complaints procedure.

7. 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 1 to 5). 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.

Kate James will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements (appendices 1 to 5).

8. Pupils using mobile devices in school

We do not encourage pupils to bring mobile devices in to school. However, at times families do request this due to split parent families. If this is the case, parents have to seek permission from the school's SHE committee. Once permission is granted, pupils should hand their device into the school office at the beginning of the school day and collect it at the end of the day.

9. 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
- › Devices lock after 2 minutes of being inactive
- › Not sharing the device among family or friends
- › Keeping operating systems up to date by always installing the latest updates

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 4).

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 the computing subject leader.

10. Learner passwords:

As a school we allocate individual usernames and passwords to pupils from KS2. Class logins are utilised for Foundation Stage and KS1 (However all pupils have their own passwords to access programmes/platforms such as Purple Mash/My Maths/SPAG.com/ IDL and Times Tables Rock Stars which are given out at the beginning of each school year along with a parent letter detailing this information to support with homework). As a school we are aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the acceptable use agreement for EYFS/KS1 and as such train staff in controlled use and monitoring to work in counteracting this.

Records of learner usernames and passwords for foundation phase students/pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.

Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.

Password requirements for pupils at Key Stage 2 and above should increase as students'/pupils progress through school.

Users will be required to change their password if it is compromised.

Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

11. 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 policies on behaviour and ICT and internet acceptable use. 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 or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident (see appendix 7).

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

12. 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 DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills 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 child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An example incident report log can be found in appendix 6.

This policy will be reviewed every year by the computing subject leader. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

15. Filtering and Monitoring – in line with KCSIE 2023 updates

Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Kate James (PREVENT lead and DSL) is in charge of ensuring filtering and monitoring is checked and updated regularly.

At Singleton School, our filtering system is called 'netsweeper'. This blocks access to harmful websites and content. Our monitoring system identifies when a user accesses or searches for certain types of harmful content on a school device.

Monthly reports (suspicious search and PREVENT) are emailed to Kate James and office staff. These are checked and actioned upon where necessary. If content has been denied, Kate James and Amanda Clayton will identify the user and act accordingly.

Suspicious search and PREVENT reports are kept in a locked cupboard in the main office. Additionally, these reports are checked by school Governors on a monthly basis.

All staff are aware that it is part of their role to monitor pupils' screens during lesson time. Staff report any concerns to Kate James and Amanda Clayton. If deemed necessary, staff will confiscate electronic devices as referenced in clause 6.3.

Each month, Kate James carries out 'on the spot' internet searches to check the validity of our filtering system. A print screen of these checks is printed and kept in a folder with the suspicious and PREVENT reports.

Appendix 1

Singleton Church of England Primary School



Pupil Acceptable Use Agreement (Foundation / KS1)

This is how we stay safe when we use computers:

1. I will ask a teacher or suitable adult if I want to use the computers / tablets.
2. I will only use activities that a teacher or suitable adult has told or allowed me to use.
3. I will take care of the computer and other equipment.
4. I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
5. I will tell a teacher or suitable adult if I see something that upsets me on the screen.
6. I know that if I break the rules, I might not be allowed to use a computer / tablet.

Signed (child):

Signed (parent):



Singleton Church of England Primary School

ICT Acceptable Use Policy (AUP) - Pupils Agreement / Internet Safety Rules

Pupil Acceptable Use Agreement (KS2)

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

- I understand that **Singleton C of E School** will monitor my use of the systems, devices, and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that **Singleton C of E School's** systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the **Singleton C of E School's** systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

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

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

- I understand that **Singleton C of E School** also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood, and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems. (Schools / academies will need to decide if they require students / pupils to sign, or whether they wish to simply make them aware through education programmes / awareness raising).

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

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g., mobile phones, gaming devices USB devices, cameras etc.

- I use my own equipment out of the school in a way that is related to me being a member of this *school / academy* e.g., communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil:

Group / Class:

Date:

Signed (child):

Signed (parent):

Appendix 3

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. A copy of the *student/pupil* acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Either: (KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent/Carers Name:

Student/Pupil Name:

Signed:

Date:

Data Protection Information:

This form is printed.

Only the Head Teacher/DSL- Amanda Clayton; Internet Safety Officer, Kate James, and Data Protection Officer- Rachel Reeves have access to these forms.

This form will be stored in a secure cabinet.

This form will be stored for the duration of the time that your child attends our school and then will be destroyed.

This form will be shredded once your child has left the school.

Appendix 4

Acceptable Use Agreement: Staff, Governors and Visitors

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems. I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8:30am and 5:30pm, except in the staff room and where there are signs to indicate this.
- I understand that personal devices with cameras on are not allowed in the classroom – these can be left safely in the school office and accessed during breaks in the staff workroom areas.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within my breaks as per the rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g., on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies. (schools / academies should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. All communications with students / pupils and parents / carers should be made via school devices. Please note the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school / academy*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems to communicate professionally. I will always use my school email for this purpose. Staff are allowed the use of staff personal email addresses on the premises during breaks and directed time.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without prior permission from the SHE committee.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school / academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

Appendix 5

Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Data Protection Information:

This form is printed.

Only the Head Teacher/DSL- Amanda Clayton; Internet Safety Officer, Kate James and Data Protection Officer- Rachel Reeves have access to these forms.

This form will be stored in a secure cabinet.

This form will be stored for the duration of the time that your child attends our school and then will be destroyed.

This form will be shredded once your child has left the school.

Name: Signed: Date:

Appendix 6: example online safety incident report log

January 2023						
Date & time	Name of pupil or staff member	Male or female	Room/computer/device number	Details of incident (including evidence)	Actions taken	Signatures 1. DSL 2. Computing coordinator 3. SHE committee
February 2023						

Appendix 7: Responding to incidents of misuse

