

Online Safety Policy

Glade Primary School



Reviewed January 2022

Next review date January 2023

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety.....	5
5. Educating pupils about online safety.....	6
6. Cyber-bullying.....	6
7. Acceptable use of the internet in school.....	7
8. Pupils using mobile devices outside school.....	7
9. Staff using work devices outside school.....	8
10. How the school will respond to issues of misuse.....	8
11. Training.....	8
12. Monitoring arrangements.....	9
13. Links with other policies.....	8
Appendix 1: acceptable use agreement (pupils and parents/carers).....	9
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors.....	10
Appendix 3: online safety training needs - self-audit for staff.....	11
Appendix 4: online safety incident report log.....	12

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. 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](#).

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 ICT Leader Hamida Miah and in liaison with the ICT Manager Kevin Crouch the designated safeguarding lead or deputies, Farzana Hussain, Sue Jones, Denise Graham or Philip Merchant.

The governor who oversees online safety is Neil Woodward (ICT) and David Hartshorn (Safeguarding)

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)

3.2 The headteacher

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

3.3 The designated safeguarding lead

Farzana Hussain is the school's DSL. Deputy DSL's are Philip Merchant, Sue Jones and Denise Graham. The E-Safety lead is Hamida Miah supported by Kevin Crouch.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- 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.

3.4 The ICT manager

The ICT Manager, Kevin Crouch is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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
- Support staff with the use of Zoom as a main tool for home learning.

This list is not intended to be exhaustive.

3.5 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 and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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
- Adhering a to the terms of using zoom as part of homeschool learning.

This list is not intended to be exhaustive.

3.6 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 1)

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 factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-og-17.pdf>
- Parentzone. <https://parentzone.org.uk/>

3.7 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, 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).

4. 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about Online Safety

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

Online safety will also be covered during parents' workshops and regular newsletters.

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and Anti-bullying 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. Class teachers will discuss cyber-bullying with their pupils and the issue will be addressed in assemblies.

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 11 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 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.

6.3 Examining electronic devices

School staff have the 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 senior leadership team 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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, staff, volunteers and governors using the school ICT system are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors and will be expected to read and agree to the school's terms on acceptable use if relevant. Parents are expected to read the parent agreement policy and children's agreement policy.

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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils are not authorised to use mobile phones on the school site.

In Y6 some pupils walk to and from school independently and for safety purposes have a mobile phone. The phone is switched off on arrival and stored in the school office until collection at home time.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

Remote and Homelearning:

Key responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the [20 Safeguarding Principles for Remote Lessons](#) infographic which applies to all online learning
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)

- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this [Online Reputation](#) guidance for schools.

Where the school has undertaken 'Zoom' as a tool for homeschooling during the pandemic. Teachers, staff and parents have a separate detailed policy agreement.

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 the 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 system or the internet, or misuses 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).

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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed Biennially by the ICT Leader. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Acceptable use policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- R.S.H.E curriculum and policy

Appendix 1: acceptable use agreement (pupils and parents/carers) – A child friendly agreement has been created for KS1 and KS2.

KS1 Agreement

My name is _____

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

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

✓

My trusted adults are:

_____ at school

_____ at home

KS2 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, including when I'm using them at home.
2. ***I learn even when I can't go to school because of coronavirus*** – 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 or 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.
3. ***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.
4. ***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, and I remember my Digital 5 A Day.
5. ***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.
6. ***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!
7. ***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.
8. ***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.
9. ***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.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
11. ***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.
12. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
13. ***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.
14. ***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.
15. ***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.

16. ***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.
17. ***I follow age rules*** – 13+ games and apps aren’t good for me so I don’t use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.
18. ***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.
19. ***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).
20. ***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.
21. ***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.
22. ***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.
23. ***I respect people’s work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***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.

~~~~~

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

**If I have any questions, I will speak to a trusted adult: at school that includes**

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

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

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

## Parents - Acceptable Use Policy

1. I understand that Glade Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school with this and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's expectations when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet (see advice in the Online Safety Policy).
9. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he may be subject to sanctions if s/he does not follow these rules.
10. I can talk to the Headteacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

**I/we have read, understood and agreed to this policy.**

**Signature/s:**

**Name/s of parent / guardian: Parent / guardian of:**

**Date:**

---

## Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

### Acceptable Use Policy (AUP): Staff and Governors agreement form

|                               |                             |
|-------------------------------|-----------------------------|
| <b>Name of School</b>         | <b>Glade Primary School</b> |
| <b>Date of next Review</b>    | <b>September 2022</b>       |
| <b>Who reviewed this AUP?</b> | <b>SLT and Governors</b>    |

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, 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 not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not download or save sensitive or personal data onto a personal device. I will store this data on the School Network Drive.
- I will ensure that I work in a secure environment, where my screen is not visible to others when working on sensitive or personal data.
- I will always log out when I finish working.
- I will report any data breaches to the Data Protection Officer (Rachel Banks) as soon as possible.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any confidential school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. I will not use my own phone to communicate with parents without prior approval of the Headteacher.
- I will be mindful of sending emails that contain chains of emails which compromise privacy by their content and personal information including email addresses

- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the ICT leader (Kevin Crouch.)
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive) that does not have up-to-date anti-virus software to the network / Internet and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras, tablets, laptops or other equipment for taking and transferring images of pupils or staff without permission and will not store images without consent of the data subjects.
- I will not use a mobile phone or other photographing equipment of my own to take any pictures of children.
- I will ensure that I secure ICT hardware using appropriate safety measures:  
Other items of ICT hardware e.g. dataloggers, cameras, will be secured in lockable cupboards when not in use.
- I will use cloud systems (e.g. School Network Drive) in accordance with School advice.
- 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 use school hardware for business purposes and personal purposes in a responsible way which minimises the risk of any data breaches. I understand that I will be subject to disciplinary procedures in line with our staff code of conduct and online safety policy should any breaches occur.
- 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 embed the school's online safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all in school Internet usage / and network usage can be logged and this information could be made available to the Headteacher.

#### **Within Social Networking:**

- I will not contact pupils using social media or any other means not authorised by the school.
- If any of my online activity affects students, staff or the wider community I understand that this could lead to disciplinary action.
- 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 understand that I cannot publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- I will not use school Social Networking sites for the promotion of personal financial interests, commercial ventures or personal campaigns.
- I will not breach any of the school's policies
- I will not identify myself as a representative of the school.

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

#### **Video conferencing:**

- I will be mindful of cameras and microphones whilst conducting zoom meetings.
- I will be aware of the background, I will be teaching or conducting meetings from. (Keep it **simple and plain**)

- I will adhere to the school dress code policy as in the staff handbook.
- I will be mindful that these sessions are recorded for monitoring and safeguarding.
- I will ensure that there are always 2 adults present. (In class teaching sessions)
- I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety, as well as safeguarding considerations when supporting pupils remotely.

### User Signature

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 agree to abide by all the points above.

Signature \_\_\_\_\_ Date:

Full Name \_\_\_\_\_ (printed)

Role within the school \_\_\_\_\_

## Appendix 3: online safety training needs – self-audit for staff

*Adapt this audit form to suit your needs.*

| Online safety training needs audit                                                                         |              |
|------------------------------------------------------------------------------------------------------------|--------------|
| <b>Name of staff member/volunteer:</b>                                                                     | <b>Date:</b> |
| Do you know the name of the person who has lead responsibility for online safety in school?                |              |
| Do you know what you must do if a pupil approaches you with a concern or issue?                            |              |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? |              |
| Are you familiar with the school's acceptable use agreement for pupils and parents?                        |              |
| Are you familiar with the school's approach to tackling cyber-bullying?                                    |              |

|                                                                                                                         |  |
|-------------------------------------------------------------------------------------------------------------------------|--|
| <p>Are there any areas of online safety in which you would like training/further training? Please record them here.</p> |  |
|-------------------------------------------------------------------------------------------------------------------------|--|

#### Appendix 4: Online safety incident report log

All E-Safety concerns are to be logged as part of CPOMs.

| Online safety incident report log |                               |                             |              |                                                           |
|-----------------------------------|-------------------------------|-----------------------------|--------------|-----------------------------------------------------------|
| Date                              | Where the incident took place | Description of the incident | Action taken | Name and signature of staff member recording the incident |
|                                   |                               |                             |              |                                                           |
|                                   |                               |                             |              |                                                           |

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

