Online safety policy
Lawns Park Primary School

Approved by: Governors	**Date:** February 22
Last reviewed: February 24	
Next review due by: **February 25**	

Table of 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 use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Have systems in place to ensure online safety during remote learning, for staff and pupils.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 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 the designated safeguarding lead (DSL).

The governor who oversees online safety is Donna Kellet (Chair of governors and safeguarding governor) All governors will:

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

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

Sarah Miles is the Designated Safeguarding Lead along with Simon Chapman(headteacher) , Lindsey Dean as the deputies.

The Designated Safeguarding Lead 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, computing lead, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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 and recorded on CPOMS.
- Updating and delivering staff training on online safety (appendix 4 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
- Keep staff up to date with recent developments and events that could impact upon the safety of children using technologies.

This list is not intended to be exhaustive.

3.4 The IT technician

The IT technician 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 weekly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 3), 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 on CPOMS 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 and logged on CPOMS.

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 (appendices 1 and 2)

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 factsheet - Childnet International

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 3).

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools

The curriculum content considers the 4C's of online safety, as referenced in KCSiE 2023: content, contact, conduct and commerce.

Content - anything posted online. Children and young people may be exposed to illegal, inappropriate or harmful content when online. This might include pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact - the risk of harm young people may face when interacting with other users. This includes peer pressure or seeing inappropriate commercial advertising. Adults can pose as children with the intention of grooming or exploiting a child.

Conduct - the way people behave online. Some online behaviour can increase the likelihood or even cause, harm (e.g. online bullying). Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce - the risk from online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Also applies to staff.

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

How we implement our offer for online safety

- ➢ 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
- ➢ School will use professional groups/agencies and charities to explore the risks with the pupils that can be encountered online. This may include drama, role play, shows and interactive experiences.

- There is a comprehensive PSHE curriculum with specific units covering online safety, safe use of social media, cyber bullying, personal safety.
- School has a curriculum for SRE that is compliant with the new statutory guidance.
- School responds to current local and national events and trends by implementing them into our curriculum.
- Up to date guides to promote online safety and the safe use of specific technologies are shared with staff and parents on the school website.

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 or Schoop. This policy will also be shared with parents. The school will let parents know what systems the school uses to filter and monitor online use. The school will tell parents what their children are being asked to do online (e.g. sites they need to visit or who they'll be interacting with online

Online safety will also be covered during specific parent's meetings.

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.

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 cyberbullying. 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.

School will discuss cyber bullying with the children as part of the annual antibullying week in school.

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 and the antibullying 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.

* Examining electronic devices to clarify that if a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent). The DSL will then decide what to do next, in line with the relevant guidance.

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 1-3). 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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they must be handed in and placed in the designated storage in class as soon as a pupil arrives at school. They will collect their device at the end of the day from the storage box in class. Pupils must turn off their phone as they enter the school grounds and must not turn it on again until they leave the premises. Therefore, pupils must not use their mobile device during;

- Lessons
- Clubs before or after school, or any other activities organised by the school
- School trips or residentials.

If a pupil brings their mobile device to an event out of school hours, they must turn it off and hand it to a member of staff on arrival. It will be returned when they leave the premises.

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 Mobile devices in school

Staff may bring mobile devices into school, but they must be kept turned off in a safe place away from the children. Staff must not access their phone when pupils are present. Staff must connect to the school Wifi rather than their own mobile data. Therefore, the use of the phone will be subject to our school filtering and monitoring systems. Staff can use their mobile device to access work related information but must not download onto their mobile device. It is the staff members responsibility to make sure that there is a secure password on their device.

10. 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 3.

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 and should not be used by anyone other than the staff member.

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 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 and corresponding consequences. 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.

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, child exploitation, grooming and the risks of online radicalisation.

All staff members will receive refresher training each academic year as part of the review of our child protection policy which is reviewed annually in line with KCSIE. There will also be relevant updates as required (for example through emails, e-bulletins and staff meetings). Safeguarding is a weekly agenda point at staff briefing.

All staff members have PREVENT training.

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 as part of their induction.

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 on CPOMS.

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the governing board.

14. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Whistleblowing policy
- Code of conduct
- Remote learning policy
- Technology loan agreement.

15. Children and online safety away from school during home learning

This includes, but is not limited to the following.

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Using inappropriate or offensive language
- Open any attachments in emails, or follow any links in emails, without first checking with an adult.
- Use any inappropriate language when communicating online, including in emails or during online lessons.
- Send unpleasant messages to my teachers or my peers.
- Share my log in details with anyone other than my parent.
- Arrange to meet anyone offline, without first consulting my parent/carer.
- Only access sites during home learning as directed by school staff.
- Wear suitable clothing and ask other members of my household helping me to do the same.
- Make sure I am working in a space where I will not be disturbed by others in my household.
- I will immediately inform school if I find any material which might upset, distress or harm me or others. This includes the reporting of unpleasant messages.

Our acceptable use policy in appendix one and appendix two, details how pupils can keep themselves safe online at home and at school. Details can also be found in our remote learning policy and in our IT loan agreement.

16. Staff and online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the Guidance for safer working practice for those working with children and young people in education settings (National Safer Recruitment Consortium May 2019).

Lawns Park Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

All parents who use school equipment at home will be expected to agree to and sign a loan agreement. See appendix

Should the need arise to deliver virtual lessons, especially where webcams/cameras are involved:

- No 1:1s, groups only. Use the lobby system and only invite children in once there are two waiting. In cases where 1:1 tuition is essential, staff must seek formal written agreement from a senior manager and the pupil's parent.
- Staff must wear suitable clothing, as should anyone else in the household.
- Find a space/room where you will not be disturbed by others in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held · Use usual school routines for sharing safeguarding concerns and non attendance.

Appendix 1: Whole School acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) I will • Ask a teacher or adult if I can do so before using them • Only use websites and apps that a teacher or adult has told me or allowed me to use. • Tell my teacher immediately if: ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • I will be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a staff member straight away if something is broken or not working properly • I understand that the school monitor, filter and check my computer files and internet sites I visit. • Let my teacher know if I hit the smoothwall immediately and what triggered it • Only use the username and password I have been given • I will not bring in memory sticks, devices, CD Roms from outside school and try to use them on the school premises. • I will not access other people's files. • Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone. • Log off or shut down a computer when I have finished using it. **If I bring a personal mobile phone into school:** • I will turn it off as I enter the school grounds and only turn it on when I leave the grounds. • Deliver my mobile phone to the office on arrival and collect it from the office at the end of the day after leaving class. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

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

Lawns Park Primary School

Acceptable Use Policy

School Policy

New technologies have become integral to everyone's lives within today's society. The internet and electronic communications technologies and the use of social media and social networks are powerful tools, which open new opportunities for everyone. However, the use of the internet and other communications technologies is a responsibility and it is **imperative** that all members of the school community are aware of the dangers of using the internet and new technologies and are clear on how they should conduct themselves.

This **Acceptable Use Policy** is intended to ensure:

- that staff and volunteers and visitors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use both in school and out of school.
- that school ICT 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 ICT in their everyday work.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email, and other digital communications though the school's filtering systems and whole school monitoring procedures
- I will log my personal device onto the school Wifi when in school. I am aware that it is for my own protection and subject to the school's monitoring and filtering systems.
- I understand that the rules set out in this agreement apply to the use of school ICT resources (e.g. laptops, i pads, email, shared areas, learning platforms and school websites) in and out of school.
- I understand that the school ICT systems are intended for educational purposes.
- I will use a password for school equipment/systems and will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate, or harmful material or incident to the appropriate person – Headteacher/ Designated safeguarding staff.
- My mobile device will be stored securely away from the children and I will not access the device with children present.
- Although I can access school emails on my personal device, I will not download professional documentation onto a personal device.

I will be professional in my communications and actions.

- 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 ensure that when I take and / or publish images of others, I will do so with their consent in line with the school's data protection policy.

- Any photographs taken on school mobile devices will be transferred swiftly on to the school network.
- I will only share images with other named agencies when there is such consent in place.
- I will never use my mobile phone to capture images or my own personal equipment.
- I will use discretion when taking images of children participating in sport so that their rights to personal privacy are not compromised.
- I will log out of sites on a personal computer or mobile device.
- I will not share email addresses, phone numbers or social identities with pupils at all.
- Any event of cyber bullying I will report to senior leaders at the first instance.
- ***Social media and networks***
- I will not use chat and social networking sites in school on any device.
- I will not access chat and social networking sites on school devices in or out of school.
- I will ensure that as a professional my use of social networking is respectful, always in line with the school's code of conduct policy. Meaning I will not post racist, radical, homophobic, or pornographic comments or materials online.
- In the run up to elections I will not post my opinions on social media or chat sites.
- I will only communicate with students / pupils and parents / carers using official school systems such as the website, schoop, email, school phone, Microsoft TEAMS or face to face.
- I will not communicate with pupils on social web sites, such as Facebook, and I will not add them to my community of friends or contacts, unless they are members of my own family.
- If a child tries to contact me on social media, I will turn down the request – let the DSL know and contact the parent in school time.
- I will ensure that any communication that takes place with parents on social web sites, who are friends socially, is purely for **personal** use, and does not compromise the school's policy on confidentiality.
- I will not use pupil names when communicating through email.
- I will not make comments (whether you have enabled privacy settings or otherwise) about my current employers or past employers or colleagues.
- I will be responsible for security and privacy settings when using social media via any chosen piece of equipment.
- I will regularly check security settings on social media sites and consider how much information I am sharing about myself and who has access to it.
- I will not refer, to my place of work on social media sites, indeed list it at all.
- I will not express opinions about my role in the school on social web sites.
- Only post comments, videos, and pictures which you would be happy to share with any groups of friends or colleagues.

Equipment use

When I use equipment loaned to me by school to carry out my professional duties, I accept that the care and use of the equipment is my personal responsibility. I will keep my computer virus checker up to date. I will carry out the maintenance procedures agreed on first receiving the computer. I will handle it with care and immediately report any problems to the technician.

- **I will not allow my friends, children and other members of my family or social network to use my school laptop and memory stick for any reason. I will ensure that information on my laptop is kept confidential and secure.**
- **I will not access social media sites using school equipment in school or at home.**

- **I will not store personal information such as personal photos on a school laptop.**
- **Only secure and authorised systems should be used to store or transfer confidential information about pupils.**
- **If I connect my laptop to the Internet at home, I will ensure that it is used appropriately, as if I was in school, and that my virus system is up to date.**
- **I will back up vital documents and information regularly.**
- **I will not leave laptops and other ICT equipment in a vehicle overnight and I will never leave school ICT equipment in sight, where it might be damaged or stolen.**
- **I understand that I am accountable for the way that school equipment is handled, stored, and used outside of the school.**
- **I will not use a personal phone to contact parents or pupils, unless it is an emergency and then I will hide my personal number. I will delete the parents, number from my call log.**
- **I will have access security on a personal phone brought into school.**
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs. I will be vigilant, at all times when opening emails.
- I will not try to upload, download or access or attempt to access inappropriate materials including but not limited to material of a violent or radical nature, 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 programs 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 only legally install additional software, for which I have a suitable licence.
- I understand that data protection 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 policy to disclose such information to an appropriate authority.

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).

Remote learning

- Avoid being online with a pupil alone. Instead use the lobby system and only invite children in once there are two waiting. In cases where 1:1 tuition is essential; staff must seek formal written agreement from a senior manager and the pupil's parent.
- Staff must wear suitable clothing, as should anyone else in the household.
- Find a space/room where you will not be disturbed by others in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held

- **I understand that I am responsible for my actions in and out of school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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 ICT 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	