MAPLE TREE PRIMARY SCHOOL
Climbing the branches of success

# Online Safety Policy

*Including Acceptable Use Agreements*

| | | |
|---|---|---|
| **Approved by:** | Senior Leadership Team | **Date:** September 2021 |
| **Last reviewed on:** | September 2021 | |
| **Next review due by:** | September 2023 | |

## Contents



## 1. Aims and introduction

Maple Tree Lower School recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

**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

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – 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 scam

## 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 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).

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 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

### 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 (DSL)

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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 support service and 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 on myconcern 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

This list is not intended to be exhaustive.

### 3.4 The ICT support service

The ICT support service 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 with the DSL and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are passed on to a DSL, to be dealt with appropriately in line with the school behaviour policy

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 myconcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are passed on to a DSL, to be dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Safeguard their child appropriately outside of school by monitoring and supporting their use of online devices
- 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)
- Alert the school to any online safety concerns involving their child immediately
- Follow the acceptable use policy themselves, especially in regard to photographs
- Approach the school directly to express any concerns rather than posting online

Parents can seek further guidance on keeping children safe online from the following organisations on our school website.

### 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.

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
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- That they are responsible for how they behave and the actions that they take online, regardless of others.

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 through newsletters, letters or other communications home, and in information via our website. There will also be opportunity for internet safety evenings and time for discussion during parents' evenings. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the deputy head. 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.) We define bullying using the acronym STOP, which stands for **S**everal **T**imes **O**n **P**urpose.

## 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. Teachers will discuss cyber-bullying with their classes as part of their PSHE and Computing lessons.

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

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

### 7.1 Acceptable Use Agreements

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

We will monitor the internet useage by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the below.

### 7.2 Email

Staff and governors should use a school email account for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to the office or senior leadership team.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

### 7.3 Visiting websites and downloading

Staff will:

- Preview sites, software and apps before their use in school or before recommending them to pupils.
- Consult with the Data Protection overseers with details of the site/service, before using any online service that requires user accounts to be created or the sharing of any personal data.
- Suggest specific websites, previously checked by the teacher, if internet research is set for homework.
- Only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

- Ensure that when working with pupils, searching for images should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine.

All users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
    - Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
    - Adult material that breaches the Obscene Publications Act in the UK
    - Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
    - Promoting hatred against any individual or group from the protected characteristics above
    - Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
    - Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Head or Deputy Head.

## 7.4 Images and videos

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers, which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to a limited range of staff. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR policy. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

## 7.5 Use of personal devices (including phones)

### 7.5.1 Staff and other adults

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas, during their breaks, and never in the presence of pupils Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device. Personal mobiles must never be used to access school emails and data. Personal devices should never be used to discuss school business. Staff may wear smart watches or exercise trackers but these should not be linked to any messages from their phone that may 'flash up' on screen.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Head teacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be on silent and out of sight.

All users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

**7.5.2 Pupils**

Pupils in Upper Key Stage 2 may bring mobile devices into school but they are not permitted to use them during the school day. The phones must be switched off on arrival and stored by the class teacher. Pupils may wear smart watches or exercise trackers to school, but these must not be linked to their personal devices or have online access. The school is not responsible for the loss, damage or theft on school premises of any personal device.

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.

## 8. Staff using work devices outside school

All staff members will take appropriate steps to ensure their work 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). Passwords must not be shared with other users and should be updated every 90 days.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install 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 3.

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 ICT support service.

## 9. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems 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. 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.

## 10. 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 the risks up
- 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.

## 11. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety through myconcern, which the DSLs monitor.

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

## 12. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Data protection policy and privacy notices

Complaints procedure

# Appendix 1 EYFS and KS1 acceptable use agreement for pupils and parents/carers

## EYFS and KS1 acceptable use agreement

Dear Parents/Carers,

The online world has become an important part of learning and life and we want all children to be safe and responsible when using any IT. Therefore, it is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules.

Please return the signed sections of this form which will be kept on record at the school.

| 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) and get onto the internet in school I will:**<br>• Ask a teacher or adult if I can do so before using them<br>• Only use websites that a teacher or adult has told me or allowed me to use<br>• Tell my teacher immediately if:<br>  ○ I click on a website by mistake<br>  ○ I receive messages from people I don't know<br>  ○ I find anything that may upset or harm me or my friends<br>• Use school computers for school work only<br>• I will be kind to others and not upset or be rude to them<br>• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly<br>• Only use the username and password I have been given<br>• Try my hardest to remember my username and password<br>• Never share my password with anyone, including my friends.<br>• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer<br>• Never share personal information (usernames, phone numbers etc) of my friends without their permission<br>• Save my work on the school network<br>• Check with my teacher before I print anything<br>• Log off or shut down a computer when I have finished using it<br>**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/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

| **Signed (parent/carer):** | **Date:** |
| --- | --- |
| | |

## Appendix 2: KS2 acceptable use agreement for pupils and parents/carers

### KS2 acceptable use agreement

Dear Parents/Carers,

The online world has become an important part of learning and life and we want all children to be safe and responsible when using any IT. Therefore, it is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules.

Please return the signed sections of this form which will be kept on record at the school.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Promote the school values in how I behave online, showing respect towards all
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Never share personal information (usernames, phone numbers etc) of my friends without their permission
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online
- Upload any photos or videos of myself or others without adults' permission
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Lie about my age in order to access games, apps or social networks that are for older people

**If I bring a personal mobile phone or other personal electronic device into school:**

- I will not use it during the school day, without a teacher's permission
- I will switch it off and give it to my teacher on arrival to school
- I will not use it to take photos while on the school site

Other devices connected to the internet:

- I will not use any devices connected to the internet (smart watches) throughout the school day
- I understand that if I break these rules, my device will be confiscated.

**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/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

| **Signed (parent/carer):** | **Date:** |
|---|---|

## Appendix 3: acceptable use agreement for staff, governors, volunteers, contractors and visitors

### Adult acceptable use agreement

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the head teacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

**Name of adult:**

- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.
- I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or Head teacher and log on myconcern.
- I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.
- If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Deputy Head or Head teacher.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

Online conduct

- Access, or attempt to access inappropriate material, including but not limited to: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Deputy Head or School Business Manager.
- Use the school's ICT systems and access the internet in school, or outside school on a work device, for anything other than educational purposes or for the purpose of fulfilling the duties of my role.
- Use devices in any way which could harm the school's reputation
- Give out my personal contact and online account information such as phone numbers, email

address, and social media account details to pupils and/or parents/carers.

- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs, videos or voice recordings of staff, pupils or anyone without checking for the necessary consent first. Where consent is given, these are to be on school devices only.
- Share confidential information about the school, its pupils or staff, or other members of the community
- Use my school email for anything other than school business, or discuss school business on any personal accounts.
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Use my personal devices in front of the children, or during lesson time, unless I have permission from the headteacher.

**When using personal devices and the internet outside of work, I will not:**

- Become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.
- Become 'friends' with any ex-pupil under the age of 13 years old and will be mindful of children older than this that they may be classed as vulnerable whilst still of school age.
- Have my social media settings set to public.
- Upload any material about or references to the school or its community on my personal social networks, including anything that undermines or disparages the school, its staff, governors, parents/carers or pupils.
- Share any priviledged information.

| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |
| --- | --- |
| I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms either:<br>• part of the terms and conditions set out in my contract of employment (staff members only);<br>• or part of my company/educational setting/organisation's contract with the school (supply, volunteers, contractors, student teachers etc);<br>• and/or my responsibilities as a governor. | |