Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

*'Caring, Sharing and Learning Together'*

# Acceptable Use Policy
# Online Safety

## Contents


| | |
|---|---|
| 1. Aims | 2 |
| 2. Legislation and guidance | 2 |
| 3. Roles and Responsibilities | 3 - 4 |
| 4. Educating Pupils about online safety | 5 |
| 5. Educating parents/carers about online safety | 5 |
| 6. Cyber-bullying | 5-7 |
| 7. Acceptable Use of the internet in school | 7 |
| 8. Pupils using mobile devices in school | 7 |
| 9. Staff using work devices outside school | 7 |
| 10. How the school will respond to issues of misuse | 7 |
| 11. Training | 8 |
| 12. Monitoring arrangements | 8 |
| 13. Links with other policies | 8 |
| **Appendix 1:** Early Years and Key Stage 1 (0-6) Acceptable Use Policy | 9 - 10 |
| **Appendix 2:** Key Stage 2 (7-11) Acceptable Use Policy | 11 - 12 |
| **Appendix 3:** Parent Acceptable Use Letter and Acknowledgement Form | 13 - 15 |
| **Appendix 4:** Staff Acceptable Use Policy and Acknowledgement Form | 16 - 23 |
| **Appendix 5:** Wi-fi Acceptable Use Policy and Acknowledgement Form | 24 - 25 |
| **Appendix 6:** PTA Social Networking Acceptable Use Policy and Acknowledgement Form | 26 - 27 |
| **Appendix 7:** Remote Learning Acceptable Use Policy | 28 - 29 |
| **Appendix 8:** Staff Social Networking Acceptable Use Policy | 30 |
| **Appendix 9:** Online Safety Incident Report Log | 31 |


## 1. Aims

Our school aims:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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

**The 4 key categories of risk**

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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 scams

## 2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2023, 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 headteachers to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

If applicable, add: The governor who oversees online safety is Stephen Hall.

All governors will:

- Ensure 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 online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 3.2 The headteachers

The headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school – this can be delegated to the DSL.

### 3.3 The designated safeguarding leads

Details of the school's designated safeguarding leads (DSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The DSLs take lead responsibility for online safety in school, in particular:

- Supporting the headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteachers and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks – for further details please see Child Protection Policy.
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteachers, ICT manager 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's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and incident report log (see appendix 9) 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 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### 3.4 The ICT manager (ICT networks)

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems on school devices and school networks, which are updated on a regular basis to assess effectiveness 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 fortnightly 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 (CPOMS and spreadsheet – Appendix 9) 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 within scope of contract with Leigh Primary School. ICT Networks does not take responsibility for working directly with children or parents during incidents but supporting school staff with filtering, monitoring and data collection related to the incident.

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 4/56/7/8), and ensuring that pupils follow the school's terms on acceptable use (appendix 1/2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting on CPOMS
- Following the correct procedures, if they need to bypass the filtering and monitoring systems for educational purposes by making a request to the headteachers who will assess risk and contact ICT networks.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 9) 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 This list is not intended to be exhaustive.
- 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:

- Notify a member of staff or the headteachers 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 1/2/3)

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

- ✓ What are the issues? – UK Safer Internet Centre
- ✓ Hot topics – Childnet International
- ✓ Parent resource sheet – Childnet International

### 3.7 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 4/5).

## 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

Online Safety is explicitly taught through:

- SRE and Health Education and PSHE using Kapow schemes of learning
- Internet Matters online curriculum
- Purple Mash Online Safety Units
- Raising awareness through Votes for Schools scheme of learning used for self-reflection in Collective Worship and assembly
- Sharing current online safety information with the parent and student community in newsletters

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

## 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 and we will inform parents through our policy and website what systems we use to filter and monitor online use and what their children are being asked to do online, including sites they will be asked to access and who if anyone their child will be interacting with online. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteachers and/or the DSLs. Concerns or queries about this policy can be raised with the headteachers or DSLs.

Parents are supported with their online safety understanding and strategies to keep children safe by:

- All having access to National Online Safety Portal
- Awareness is raised weekly in the Leigh Latest with a suggested guide and webinar to watch
- Website information on policy, helpful links and stories to read with young children

## 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.)

### 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 classes, and through explicit teaching and the issue will be addressed in assemblies/votes for schools.

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.

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 DSLs 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices).

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 3-8.

## 8. Pupils using mobile devices in school

Only Year 6 Pupils may bring mobile devices into school, but are not permitted to use them. They are to be handed to the school office turned off at the start of the day and must be password protected. They can be collected at the end of the day by the children for purposes of safety when they leave the premises.

Any breach of the above will result in confiscation of their device and it will be returned to the parent/child at the end of the day. Parents will be notified of the breach.

## 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 4.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. Passwords must have 8 characters, with a combination of upper and lower case letters, numbers and a special character.
- 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.
- The hard drives of all work laptops are encrypted by our ICT network company to ensure that no one can access the files stores on the hard drive by attaching it to a new device. All devices have anti=virus and anti-spyware software installed upon them. It is the responsibility of the school ICT network services to update systems with the latest updates to operating systems.
- The device must not be shared with family or friends.
- Devices must not be left inactive for a period of time and unlocked.
- The device should be used solely for work activities.
- If staff have any concerns over the security of their device they must seek advice from the DSL and ICT network services.

## 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 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 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 deputy 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.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

## 12. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety on CPOMS as well as on an incident report log (appendix 9). This policy will be reviewed annually by the Headteachers. 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 policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Mobile and SMART technology policy
- Image Use Policy

# Appendix 1

# Early Years and Key Stage 1 (0-6)
# Acceptable Use Policy

## Statements to be used in school with the children:

I understand that the Leigh Primary School Acceptable Use policy will help keep me safe and happy online.

- I only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online when I use a computer, tablet or Chrome book.
- I know that if I do not follow the rules then:
    - My computer will be turned off
    - Mrs Halfhide/Mrs Shobbrook will speak to me and if needed they will speak to my parents or guardians
- I have read and talked about these rules with my parents/carers
- I always tell an adult/teacher if something online makes me feel unhappy or worried.
- I can visit www.thinkuknow.co.uk and www.ceopeducation.co.uk to learn more about keeping safe online

# Early Years and KS1 Acceptable Use Poster

**Appendix 2**

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP

Telephone/Fax: 01732 832660

# Key Stage 2 (7-11) - Acceptable Use Policy

## Statements to be used in school:

I understand that the Leigh Primary School Acceptable Use policy will help keep me safe and happy online.

**Safe**

- I will be kind and respectful online, just like I am in school.
- I will only share pictures or videos on the internet if they are safe, kind, and I have asked for permission first.
- I will only chat with people I know online, or I will ask a safe adult to help me decide if someone I don't know is safe to speak with online.
- I only click on links if I know what they do, or I will ask a safe adult first.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will not agree, I will immediately talk to an adult first.

**Learning**

- I know I am not allowed my own personal smart devices and/or mobile phone at school/setting and if I need to bring one I must request permission from a teacher.
- If I have permission to being in a personal device, I know it must be handed into the office in the morning and collected at the end of the day.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen or given me permission to use.
- I use school/setting devices for school/setting work unless I have permission otherwise.
- If I need to learn online at home, I will follow the school/setting remote learning AUP.

**True**

- I know that some things or people online might not be honest or truthful.
- If I'm unsure if something online is true, I will check other websites, books, or ask a safe adult.
- I always credit the person or source that created any work, images, or text I use.
- I will only use Artificial Intelligence (AI) tools when [my teacher/ a safe adult] says it is allowed
- I will not put personal information about me or anyone else into AI tools. I will not use AI to make fake images, voices, videos or messages about other people.

**Responsible**

- I use school computers for school work, unless I have permission otherwise
- I keep my personal information safe and private online including: m address, my telephone number or pictures of myself or family.
- I will not pretend to be anyone else online and I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will keep my passwords safe and not share them with anyone. When I am finished, I will log of the computer fully before closing down.
- I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher/technician has allowed me to
- If I bring in a CD or memory stick I will give it to my teacher first so it can be checked for viruses before it is inserted into a computer.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these, I should report it to a teacher or adult in school, or a parent or carer at home.

**Understand**

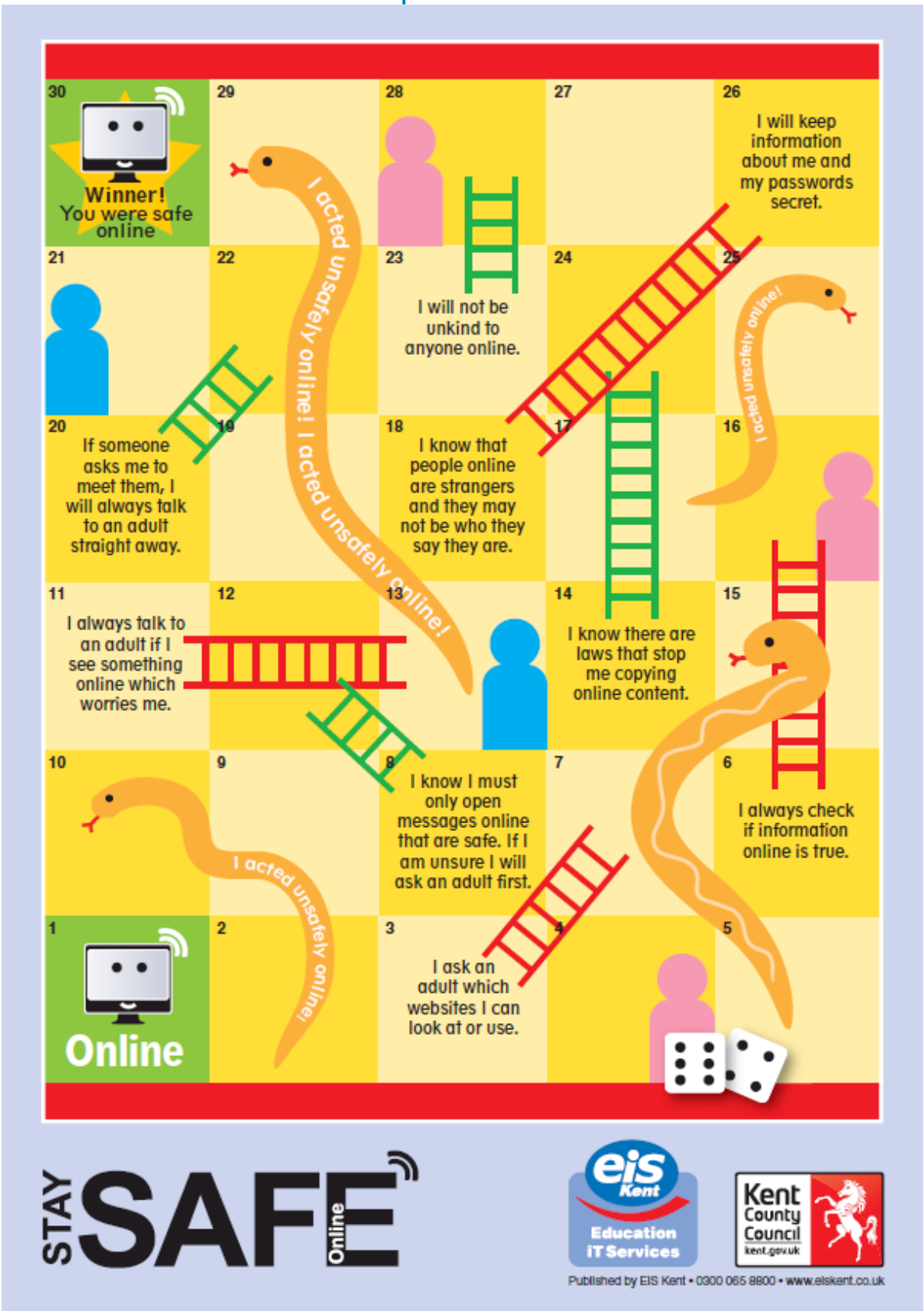
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored. I know that school online platforms are monitored when I am at home.
- I have read and talked about these rules with my parents/carers
- I understand that my behaviour online can affect others and I will not behave in a way that will upset, frighten or embarrass others.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online
- I know that if I do not follow the school rules then:
    - My computer will be turned off
    - Mrs Halfhide/Mrs Shobbrook will speak to me and if needed they will speak to my parents or guardians

**Tell**

- If I am aware of anyone being unsafe with technology then I will report it to a teacher
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried, sad or frightened.

- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page/shut the lid of my laptop/Chromebook and tell an adult straight away. The adult may then turn off my computer or make sure any unsafe content is removed/reported.
- I know it is not my fault if I see or someone sends me something bad online.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- I understand that the adults at [school/setting] are responsible for keeping me safe; they may need to speak to other safe adults, or my parents/carers, if I tell them about something that has happened online.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help.

## KS2 Acceptable Use Poster



## Appendix 3

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

Dear Parent/Carer

All pupils at Leigh Primary School use computer facilities and internet access, as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Google Platform, Purple Mash, Nessy/EdShed, SPAG.com and Doodle Learning
- Email
- Games-based technologies
- Digital cameras, web cams and video cameras

Leigh Primary School recognises the essential and important contribution that technology plays in promoting children's learning and development, believe it and offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, adhering to age restrictions, to ensure that pupils are safe when they use our internet and systems.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child, discuss the content with them and return the attached slip.

For Reception and Key Stage 1 children we understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful way to achieve this.

Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website's http://www.leighprimaryschool.com/ for more information about our approach to online safety. Full details of the school's online safety policy are available on the school website http://www.leighprimaryschool.com/Policies/ or on request. All families have access to National Online Safety which is a portal which provides advice, guidance, webinars, training and support regarding all aspects of Online Safety pertaining to the 4 main areas of risk:

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

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact the school Designated Safeguarding Lead Mrs Shobbrook or myself.

Yours sincerely,
Jenna Halfhide (Co-Headteacher)
Joanne Shobbrook (Co-Headteacher)

*Leigh Primary School*

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

# Parent/Carer Acceptable Use Policy Acknowledgement Form

**Pupil Acceptable Use Policy: Leigh Primary School Parental Acknowledgment**

I, with my child/children have read and discussed Leigh Primary School's Acceptable Use Policy which can be found in the policy section of the school website. I understand that the AUP will help keep my children safe online and applies to my child's use of school devices, systems and platforms on sites and at home and personal use where there are safeguarding or behaviour concerns. This could include online behaviour which poses a threat or causes harm to another child/pupil and could have repercussions for the orderly running of the school setting and if behaviour could adversely affect the reputation of the school.

I am aware that any internet and computer use using school equipment are filtered and may be monitored for safety and security reasons to safeguard both my child and the school's systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I am aware that any use of children's personal devices/smart technology is prohibited on site e.g. mobile phones and tablets.

I understand that my child needs a safe and appropriate space to access remote learning if the school/setting is closed in response to any given emergency situation. I will ensure my child's access to removed learning is appropriately supervised and any use is in accordance with the School Acceptable Use Policy.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

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

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations, if I have concerns over my child's or other members of the school communities' safety online for example: speaking the schools DSLs or another member of staff.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools online ssafety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home appropriate to their age and understanding. I will use appropriate parental controls, supervise access and school online safety communications to support my understanding of advances in technology in order to keep my child safe.

I know I can also visit the following website for support with online safety: www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org, www.saferinternet.org.uk, www.childnet.com and https://nationalonlinesafety.com/

**Please inform the school that you have read this policy through Arbor consent.**

## Appendix 4

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

Dear All members of staff

At Leigh Primary School we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at Leigh Primary School take precautions in order to protect themselves both professionally and personally online. With this in mind, we request that all members of staff:

- **Take responsibility for their mobile and smart technologies as well as work devices:**
  - We recognise that technologies of this type are part of everyday life and all devices brought onto site are the responsibility of the user and should never be used or accessible to pupils. Leigh Primary School will take no responsibility for any loss, theft or damage of personal devices.
  - All devices should have password protection to prevent unauthorised access of 8 characters with a combination of upper- and lower-case letters, numbers and special characters.
  - Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods unless written permission has been given by the headteacher/manager, such as in emergency circumstances.
  - Do not use personal equipment for taking photos or videos of children in line with our image use policy.
  - Do not use personal accounts to communicate with children/parents.
  - Only work devices are to be used for conducting remote learning outside of work as these devices are encrypted.
  - Work related material which is confidential is not to be stored on personal devices. Any work related and confidential material is to be stored on a work device which is password protected to the described standard or in a secure business cloud-based platform. For Leigh Primary this is Office365 and CPOMS for behaviour and safeguarding information.
- **Are conscious of their own professional reputation and that of the school when online.**
  - All members of staff are strongly advised in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it.
  - Content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences. This can have consequences including civil, legal and disciplinary action being taken.
  - It is the school's expectation that staff members safeguard themselves by setting appropriate privacy settings, being aware of implications of location sharing services, opting out of public listings on social networking sites, logging out of accounts after use, using strong passwords and importantly ensuring that personal views are never presented as being that of the school regardless of that the view may be.

- We request that staff do not identify themselves as employees of Leigh Primary School on their personal social networking accounts this is to prevent information being linked with the setting and to safeguard privacy of staff members.
- Any information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or as colleagues, will not be shared or discussed on social media sites.
- Staff should not engage in excessive use of social media during school hours on personal devices or using any school device to engage in social media use at all. Social media on personal devices should only be at lunchtimes, before and after school hours. Social media is restricted by the school's systems on work devices and will result in disciplinary action.

- **Are aware that as professionals, we must ensure that the content we post online does not bring the school or our professional role into disrepute, and does not undermine professional confidence in our abilities. This is part of the teacher's standards.**
  - The teaching standards state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.
  - The sending of abusive or inappropriate messages via personal smart devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour, child protection policies and staff discipline policy as appropriate.
  - All members of the Leigh Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, contravene confidentiality or data security/protection or which would otherwise contravene our behaviour/staff code of conduct or child protection policies.
  - If a member of staff is thought to have illegal content saves or stored on a personal device or school device or have committed a criminal offence, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations against staff policy.'
  - All content/data on the Office365 platform is the property of Leigh Primary School. Therefore, information should not be downloaded on exiting the employ of the school and it is advisable not to conduct personal emails on your school account as access will be restricted on departure.

- **All Staff be careful when publishing any information, personal contact details, video or images online.**
  - It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online, but do so respectfully.
  - Ensure that the privacy settings of the social media sites that you use are set appropriately and access to restricted
  - Ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or their parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all.

- **Do not accept pupils (past or present) or their parents/carers as "friends" on a personal account unless they are employed by the school.**
  - You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns.
  - If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns, please speak to the Designated Safeguarding Lead: Jenna Halfhide and Mrs Shobbrook.
  - If a parent contacts you via a personal email or personal social media account in a work capacity, it is advisable not to respond but to confer with a member of the senior leadership team. It is also ill advised to respond in a personal and social form to any parent should a communication be made that is not work related. Communication in relation to your teaching role is through the school office and part of our communication policy.
  - **NEVER** respond to a past/present pupil communication on social media.

- Parent Whatsapp groups are included as social media channels and are not official communication channels of the school. Staff members may communicate as a parent as long as any views do not bring the school into disrepute, contravene confidentiality or form a work communication. All work communications are to be sent via the school office and NOT through Whatsapp groups, however trivial.

- **Always use a work provided email address or phone number to contact children and parents – this is essential in order to protect yourself as well as the wider community. If you use a personal device – keep your number private.**
- **If you are concerned about a child's wellbeing or online behaviour then please speak to the Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook. If you are targeted online by a member of the community or are concerned about a colleague, then please speak to the headteacher and/or chair of governors.**
  - If you are unhappy with the response you receive, or do not feel able to speak to the Designated Safeguarding Leads, headteachers or chair of governors then we request you follow our Whistleblowing procedure.
- **Always comply with school policy and acceptable use policy when using official school social media platforms.**
  - Posts on Twitter can only be made by Joanne Shobbrook and Jenna Halfhide. Staff members may email and request a share onto this platform.
  - PTA have a Facebook page – This is not an official communication channel from the school but posts can be made on behalf of the school if requests are made to the PTA. The Headteacher or Deputy Head must always be aware of any request to authorise this as an official school communication.
  - The official use of social media sites by Leigh Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the headteacher prior to use
  - Any images used should comply with parental consent which is dependent upon the platform.
  - Any post on Google Classroom should conform to our Acceptable Use Policy and be used for positivity and to celebrate all pupils equally.
  - Any website updates should be drafted and be approved/proof read by a member of the Senior Leadership Team before posting online.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practice with technology" are available in the staffroom to help you consider how to protect yourself online.

Please photocopy them if you want or download the documents directly from:

- www.childnet.com,
- www.e-safety.org.uk
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk

Additional advice and guidance for professionals is available locally through the Education Safeguarding Team or nationally through Professional Unions and/or the Professional Online Safety helpline www.saferinternet.org.uk/about/helpline

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school code of conduct could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Please speak to your line manager, the Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook if you have any queries or concerns regarding this.

Yours sincerely,

Jenna Halfhide and Joanne Shobbrook
Co-Headteachers

### *Additional regarding online participation on behalf the School*

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the school then we request that you:

- Be professional and remember that you are an ambassador for the school. Disclose your position but always make it clear that you do not necessarily speak on behalf of the school.
- Be responsible and honest at all times and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Be accountable and do not disclose information, make commitments or engage in activities on behalf of the school unless you are authorised to do so.
- Always inform your line manager, the designated safeguarding lead and/or the headteacher of any concerns such as criticism or inappropriate content posted online.

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

# Staff Acceptable Use Policy (AUP)

**As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.**

**Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff Leigh Primary School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.**

**This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.**

**Policy Scope:**

1. I understand that Leigh Primary School's AUP should be read in line with the school behaviour policy, child protection policy and Staff Handbook and Remote learning AUP. I understand that signing this Policy also means I have understood and will adhere to the guidance in the letter attached to this acknowledgement.

2. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Leigh Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

4. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

5. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational purposes/professional use.

6. Where I deliver or support remote learning, I will comply with the school/setting remote learning AUP.

**Date and System security**

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate and comply with password specific requirements set out by our ICT/Network services. I will protect the devices in my care from unapproved access or theft by not leaving them is visible and unsupervised public places.

8. I will respect system security and I will not disclose any password or security information. I will follow the school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.
9. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager. I will not open hyperlinks or attachments in emails unless they are from a known and trusted source. I will report any such emails to our IT system manager.

10. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998.
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
    - Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

11. I will not keep or access professional documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school's Office 365 platform to store work documents and files in a password protected environment.

12. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

13. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

14. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook as soon as possible.

15. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead as soon as possible.

16. Any images or videos of learners will only be used as stated in the schools use of images procedures. I understand that images of learners must always be appropriate and should only be taken with school provided equipment and only be taken/published where learners and parents have given explicit written consent.

**Classroom and Professional Practice**

17. I am aware of the expectations relating to safe technology use inb the classroom, safe remote learning and other working spaces as listed in our online safety policy, AUP, safeguarding and behaviour policy.
18. I have read and understood the school mobile and smart technology and social media policies.
19. If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider/staff, in line with the school's child protection policy.
20. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where learners feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Jenna Halfhide/Joanne Shobbrook) or a deputy (Victoria Short/Tracey Prockter) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate ,including when remote teaching, carefully considering search tools and use of AI.
21. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them
22. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism/cheating, and inaccurate, harmful and/or biased material. Additionally, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
    - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
    - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
    - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of childrens, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the DPO/leadership team has confirmed that the processing is lawful and appropriate.
    - I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
    - I will not use AI to make decisions about children, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
    - Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
    - I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the school child protection, behaviour, anti-bullying, staff conduct and data protection procedures

**Mobile phones and smart devices**

23. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff behaviour policy/code of conduct, mobile phone policy and the law.

24. I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for children.

25. Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school-provided devices where available. Where staff are permitted to use personal devices for professional purposes, this must be formally agreed by the school/setting and managed in line with [school/setting] policy.

26. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

**Online Communication including use of social media on mobile and smart technology**

27. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff behaviour policy conduct, child protection policy and the school social media policy and the law.
    - I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to learners, staff, school or parents/carers on social media.

28. My electronic communications with current and former [children/pupils/students] and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school-provided communication channels and systems, such as a [school/setting] email address, user account or telephone number.
    - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with children/students or their families, unless this has been formally approved, risk assessed and recorded by leaders.
    - I will not share any personal contact information or details with students, such as my personal address, email address or phone number.
    - I will not share personal information about my private life with students online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.
    - I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former students, or their parents/carers, where this is linked to my role, the school, or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
    - Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or headteacher. This is to help safeguard students, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
    - Where digital communication with students or families is required, I will follow the school's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

29. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Online Safety policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school code of conduct and the Law.

**Policy Concerns, compliance and breaches**

30. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.

31. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.

32. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.

33. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the headteacher, in line with the school's child protection policy, staff behaviour policy/code of conduct, low-level concerns procedures and/or allegations against staff policy.

34. If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the DSL and the headteacher.

35. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of students and staff.
    - This includes monitoring all school-provided devices and school systems and networks including school-provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
    - This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

    - Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.

36. I understand that if the school believes that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the [school/setting] may invoke its disciplinary procedures as outlined in the staff behaviour policy.

37. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL/Headteacher so it can be recorded and managed transparently.

38. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

39. I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.

40. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

41. I understand that if the school] suspects criminal offences have occurred, the police will be informed where appropriate.

42. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or headteacher before taking action. I will act in a way that safeguards students, protects professional boundaries, and is open to scrutiny.

**I have read, understood and agree to comply with Leigh Primary School Staff Acceptable Use Policy**

Name: ……..… Signed: ……....

Date: ……..…

Accepted by: ……..…… Date: ……

**Appendix 5**

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

# Wi-Fi Acceptable Use Policy

## For those using school Wi-Fi

***As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school's boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.***

1. The school provides Wi-Fi for the school community and allows access for educational use.

2. Use of the Wi-Fi falls under Leigh Primary School's Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All students, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.

3. The school reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.

4. School owned information systems, including Wi-Fi, must be used lawfully. I understand that the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to computer material, gain unauthorised access with intent to commit or facilitate further offences, or modify computer material without authorisation.

5. I will take reasonable steps to ensure that any personal device connected to [school/setting] Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.
6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass school security, filtering or monitoring systems, or download unauthorised software, applications or files.

7. I will not use school Wi-Fi to access, create or share illegal or harmful content, compromise another person's safety or privacy, interfere with systems, or breach relevant school policies.

8. I will not use school Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with school data protection and safeguarding procedures.

9. Staff using school Wi-Fi on personal devices remain subject to the staff behaviour policy/code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.

10. The school takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk. Where personal devices are permitted to connect to the school Wi-Fi, users do so at their own discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.

11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the Designated Safeguarding Lead – Joanne Shobbrook and Jenna Halfhide - or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL, identified technical contact or headteacher.

12. I understand that activity carried out through school Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that the school can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

13. If the [school/setting] suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant [school/setting] procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, headteacher/manager, employer/organisation, LADO or police.

**I have read, understood and agree to comply with Leigh Primary School Wi-Fi Acceptable Use Policy.**

Signed: ……..... Print Name: ……..……

Date: ……

Accepted by: ……..…. Print Name: ……..

**Appendix 6**

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

# PTA/Committee Social Networking Acceptable Use Policy

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety. I am aware that (tool using such as Facebook, Twitter) a public and global communication tool and that any content posted on the site/page/group may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook.
    - The headteacher retains the right to remove or approve content posted on behalf of the school.
    - Where it believes unauthorised and/or inappropriate use of the social media sites or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
    - Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion on social media will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of social media sites and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

6. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. The school Designated Safeguarding Lead and/or school management team will have full admin rights to the account.

7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook.

9. I will ensure that the social media site is moderated on a regular basis as agreed with the Designated Safeguarding Leads.

10. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.

11. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook.

**I have read, understood and agree to comply with Leigh Primary School PTA/committee Social Networking Acceptable Use Policy**

Signed: ……..…..... Print Name: ……

Date: ……..……

Accepted by: …….. Print Name: ……..

**Appendix 7**

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP
Telephone/Fax: 01732 832660

# Remote Learning Acceptable Use Policy (AUP)

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of Leigh Primary School community when taking part in remote learning following any full or partial closures.

**Leadership Oversight and Approval**

1. Remote learning will only take place using Google Classroom.
2. Staff will only use school managed accounts with learners and parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
    - Staff will use work provided equipment where possible e.g. a school/setting laptop, tablet, or other mobile device.
3. Online contact with remote learners and/or parents/carers will not take place outside of the operating times as defined by SLT (8am – 6pm)
4. Live-streamed remote learning sessions will only be held with approval and agreement from the headteacher/a member of SLT.

**Data Protection and Security**

5. Any personal data used by staff and captured by Google Classroom when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
6. All remote learning and any other online communication will take place in line with current confidentiality expectations set out in our Privacy Notice.
7. Staff will not record lessons or live meetings using personal equipment.
8. Only children and parents of the Leigh Primary School will be given access to Google Classroom.
9. AI note takers, transcription tools, recording bots or automated meeting summaries must not be used in remote/online learning, meetings or training unless this has been approved in advance by leaders and is managed in line with safeguarding, consent, confidentiality and data protection requirements.

**Session Management**

10. Appropriate privacy and safety settings will be used to manage access and interactions.
11. When live streaming with learners:
    - contact will be made via learners' Google Classroom
    - contact will be made via a parents/carer's account
    - staff will mute/disable learners' videos and microphones on entry to the session and release as appropriate for the lesson
    - at least 2 members of staff will be present.
    - If this is not possible, SLT approval will be sought.
12. Live 1:1 sessions will only take place with headteacher permission with appropriate risk assessment in place.

13. A pre-agreed invitation/email/message using school email or Google Classroom detailing the session expectations will be sent to those invited to attend.

- Access links should not be made public or shared by participants and this should be made clear in the invitation.
- Learners and/or parents/carers should not forward or share access links.
- Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

14. Alternative approaches and/or access will be provided to those who do not have access.
15. Staff will explain any expectations about the location from which [children/pupils/students] take part. These will reflect their age, needs, privacy, home circumstances and the nature of the session.

**Behaviour Expectations**

16. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
17. All participants are expected to behave in line with existing school policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - No participant will not take or record images for their own personal use.

18. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
19. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
20. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

**Policy Breaches and Reporting Concerns**

21. Participants are encouraged to report concerns during remote and/or live-streamed sessions:
22. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to Jenna Halfhide.
23. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
24. Sanctions for deliberate misuse may include: restricting/removing use and contacting police if a criminal offence has been committed.
25. Any safeguarding concerns will be reported to Jenna Halfhide and Joanne Shobbrook, Designated Safeguarding Lead, in line with our child protection policy.

**I have read, understood and agree to comply with Leigh Primary School's Remote Learning AUP.**

Signed: ……..... Print Name: ……

Date: ……..……

Accepted by: …….. Print Name: ……..

**Appendix 8**

Leigh Primary School

The Green, Leigh, Tonbridge, Kent TN11 8QP

Telephone/Fax: 01732 832660

# Staff Social Networking Acceptable Use Policy

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety. I am aware that Twitter and Facebook is a public and global communication tool and that any content posted may reflect on the school, its reputation and services.
2. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook. The headteacher retains the right to remove or approve content posted on behalf of the school.
4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
    - Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion on the school's social media site will not be forwarded to any other person or organisation.
6. I will promote online safety in the use of Twitter and Facebook and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by the Designated Safeguarding Leads/headteachers prior to use.
7. I will set up a specific account/profile using a school provided email address to administrate the account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Leads and/or headteachers will have full admin rights to the site and page.
8. Where it believes unauthorised and/or inappropriate use of the site or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
9. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.
10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the headteacher and/or Designated Safeguarding Leads urgently.
11. I will ensure that the site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Leads.
12. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.
13. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead Jenna Halfhide and Joanne Shobbrook.

Signed: ……..…..... Print Name: ……

Date: ……..……

Accepted by: …….. Print Name: ……..

# Appendix 9: online safety incident report log

***This is illustrative of our online log of incidents in an excel format.**

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |