BIGGIN HILL
PRIMARY SCHOOL

# Online Safety Policy

| | |
|---|---|
| Person(s) Responsible: | Headteacher/Safeguarding Link Governor |
| Formally adopted by the Governing Body: | September 2024 |
| Review date: | September 2025 |

***This policy also applies to the Early Years Foundation Stage (EYFS)***

**This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure**

## Contents

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Biggin Hill Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

**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, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (September 2024), 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 the headteacher and authorised members of staff stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on childrens' 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 body

The governing body has overall responsibility for monitoring this policy and holding the headteacher 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 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 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.

The governor who oversees online safety is Maria Daley.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school 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 SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

## 3.2 The headteacher

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

## 3.3 The designated safeguarding lead

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, 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 child protection policy
- Ensuring that any online safety incidents are logged (see appendix 7) 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 6 contains a self-audit for staff on online safety training needs which will be completed before the online safety safeguarding meeting)
- 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 Staff managing the technical environment

Staff managing the technical environment are responsible for:

- Putting in place an ‘appropriate level’ of security protection procedures, filtering and monitoring systems, which are updated on a regular basis and keep children 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 weekly basis through LGFL
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 7) 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.

## 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
- 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’

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 4), and ensuring that children follow the school's terms on acceptable use (appendices 2 and 3)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 7) 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.

### 3.6 Parents

Parents are expected to:

- Sign the school's acceptable use agreement upon admission (appendix 3)
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1-3)

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 4).

## 4. Educating children about online safety

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

In **Key Stage 1**, children 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

Children in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*

- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- *What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)' to the list of things pupils will know by the end of primary school*

Safer Internet Day is a whole school event that raises the profile of the importance of online safety. This is a day which is celebrated globally and takes place in February each year.

RSE lessons will be taught every year to every year group (YR-6) in the Summer Term.

In addition to this children will be taught age-appropriate online safety education throughout the year during PSHE lessons.

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

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

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety via the BHPS Safeguarding Bulletin.

This policy will also be shared with parents.

Online safety will also be covered during parent workshops.

The school will let parents know:

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

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

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

## 6. Acceptable use of the internet in school

All children, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-4). 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 children, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1-4.

# 7. Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

If a member of staff is made aware of an instance of cyberbullying, then the DSL will be notified. Any online safety concerns about a child/children will be logged through our usual safeguarding procedures.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.

Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.

Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Service or the Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or will speak with the Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

# 8. Procedures for Responding to Specific Online Incidents or Concerns

## 8.1 Cyber Bullying

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 school anti-bullying policy).

## 8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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 children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and the computing teacher will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support children, as part of safeguarding training (see section 12 for more detail).

The school also sends information on cyber-bullying to parents via the monthly safeguarding bulletin so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among children, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 8.3 Examining electronic devices

The headteacher and authorised members of staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on childrens' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, the headteacher and authorised members of staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

If inappropriate material is found on the device, it is up to the headteacher and authorised members of staff 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, authorised staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable.

If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

  *  **Not** view the image

  *Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of children will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

## 8.4 Artificial Intelligence (AI)

Generative artificial Intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Biggin Hill Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Biggin Hill Primary School will treat any use of AI to bully pupils in line with our Anti-Bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

## 8.5 Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood the guidance of 'Keeping Children Safe in Education (September 2024)'.

Biggin Hill Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

Biggin Hill Primary School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

Biggin Hill Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Biggin Hill Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- If content is contained on learners' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.

- o If appropriate, make a referral to partner agencies, such as Children's Social Care Service and/or the Police.
- o If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
  - ▪ If a criminal offence has been committed, the DSL (or deputy) will discuss this with the Police first to ensure that investigations are not compromised.
- o Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

### 8.6 Youth Produced Sexual Imagery ("Sexting")

Biggin Hill Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".

Biggin Hill Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- o View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

  - ▪ If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- o Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- o Act in accordance with our child protection policies and the relevant Safeguarding Child Partnership's procedures.
- o Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- o Store the device securely.
  - ▪ If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- o Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- o Inform parents and carers, if appropriate, about the incident and how it is being managed.
- o Make a referral to Children's Social Care and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- o Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.
  - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

## 8.7 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

Biggin Hill Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Biggin Hill Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

- We will ensure that the ‘Click CEOP’ report button used to report online child sexual abuse is visible and available to learners and other members of our community.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Safeguarding Children Partnership’s procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children’s Social Care Service (if required/appropriate) and immediately inform the police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

- Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or the Police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).

If learners at other settings are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

## 8.8 Indecent Images of Children (IIOC)

Biggin Hill Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Education Safeguarding Service.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant Safeguarding Children Partnership's procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), the police.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

### 8.9 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Biggin Hill Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.
All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the Police.

### 8.10 Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.

If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

## 9. Children using mobile devices in school

Year 6 children may bring mobile devices into school, but are not permitted to use them during the school day.

Any use of mobile devices in school by children must be in line with our Mobile Phone Policy for pupils (appendix 5) and the acceptable use agreement (see appendices 2-3).

Any breach of the acceptable use agreement by a child may trigger disciplinary action in line with the school behaviour policy and may result in their device being confiscated.

## 10. Staff and visitors using mobile devices in school

Members of staff or visitors are not permitted to use their own personal phones or devices for contacting learners or parents and carers. Staff or visitors will not use personal devices to take photos or videos of learners and will only use work-provided equipment for this purpose.  Any use of mobile devices in school by staff and visitors must be in line with our Mobile Phone Policy and the acceptable use agreement (see appendix 4).

If staff are asked by the Headteacher to contact children to check on their welfare during school closure and do so using their mobile phone then they should use 141 to conceal personal information.

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

## 11. 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. They must take all reasonable steps to ensure the security of their work device when using it outside school. All work must be stored in the school google drive.

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.

## 12. Remote learning - Virtual lessons and Live Streaming

Teaching from home and to childrens' homes is different from teaching in the classroom. In order to safeguard both children and staff when broadcasting a lesson or making a recording, teachers should:

- Use the school's conferencing service so that the teacher can disable users' microphone and video cameras.
- Be clear about the expectations of student behaviour (e.g. a 'classroom standard' of behaviour is expected from all participants).

- Be clear about whether it is acceptable for students to record events and expectations/restrictions about onward sharing.
- Record in a shared space and not in their bedroom (if that's not possible, use a neutral background).
- Dress like they would for school and wear their school lanyard
- If they are sharing a screen, double check that any other tabs they have open in their browser would be appropriate for a child to see.
- Avoid 1:1 tuition
- Avoid using personal devices and use school provided equipment
- If the chat function is used as part of a live lesson then it should be monitored by the staff member in charge of the lesson.
- Remind staff of safeguarding obligations. Report any safeguarding incidents or potential concerns according to the school policy.
- Remind students of who they can contact within the school for help or support.
- Ensure staff are the first to arrive and the last to leave a meeting.

Children should:

- Be in a shared space in their house, rather than in their bedroom and appropriately dressed.
- Ask parents who'll also be there to be mindful that other children might see or hear them and anything in the background.
- Follow normal school rules with respect to behaviour.
- Report any safeguarding incidents or potential concerns according to the school policy.

All children are invited to join Google Meet Live lessons by following a link on their Google Classroom home page. All live lessons are recorded for safeguarding purposes. Recordings are not made accessible after the live lesson and are stored securely within the G Suite. All recordings will be deleted after the particular period of school closure, during which the recording was made, has ended.

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

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. 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.

## 14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

## 15. Filtering and Monitoring arrangements

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

All staff, including office staff, teaching staff, primary students and IT accounts, are responsible with keeping themselves and others safe online. Biggin Hill Primary School's filtering and monitoring system can be found in appendix 8.

Filtering:

- URLs are filtered through our school's network (LGfL's WebScreen)
- WebScreen URLs are categorised as appropriate or harmful/inappropriate
- Staff, teaching staff, primary students and IT accounts have different access to different URL categories based on their need
- Appropriate categories will allow the relevant URLs to load
- Harmful/inappropriate categories are blocked and the URLs will be denied access to load

Monitoring:

- The school's web filtering and monitoring systems are checked weekly
- If any inappropriate sites are being accessed then this will be raised with staff where appropriate

Reporting:

- If a page has loaded that is thought to be deemed inappropriate, it must be reported via the SNS Report a Fault tile via RM Unify. This will be reviewed by the school's IT technician.
- If a child has accessed a site deemed inappropriate, it must be reported on My Concern, Reported as a fault via SNS Report a Fault and the Computing Lead must be notified.
- The IT technician and DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 7.

## 16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Mobile Phone Policy
- Social Media Policy

# Appendix 1: EYFS and KS1 Acceptable Use Agreement - Pupils to sign in school

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

| | |
|---|---|
| **Signed:** | **Date:** |

# Appendix 2: KS2 Acceptable Use Agreement - Pupils to sign in school

## ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

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

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

- Always use the school’s ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher’s permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I’m finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school’s network using someone else’s details
- Arrange to meet anyone offline without first consulting my parent/carer
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate

**I agree that the school will monitor the websites I visit and that there will be consequences if I don’t follow the rules.**

| | |
|---|---|
| **Signed:** | **Date:** |

## Appendix 3: Parents/carers acceptable use agreement (for Admissions form)

**Acceptable Use of the School's ICT Systems and Internet: Agreement for Parents/Carers**

As the parent or legal guardian of the above pupil, I grant permission for my son/daughter to have access to use the Internet, Google email (Gmail), Google Classroom and other ICT facilities (iPads and Chromebooks) at school.

I accept that ultimately the school cannot be held responsible for the nature or content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files and the Internet sites they visit and that if they have concerns about their e-safety or online behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns regarding my child.

I will make sure my child understands the following conditions depending on their Key Stage and I understand that my child will sign the appropriate Acceptable Use Agreement in school.

I understand that below are the conditions my son/daughter will adhere to if they are in EYFS/KS1:

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

I understand that below are the conditions my son/daughter will adhere to if they are in KS2:

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

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

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

## Appendix 4: acceptable use agreement (staff, governors, volunteers and visitors)

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

**Name of staff member/governor/volunteer/visitor:**

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Contact children/parents or take photographs of children on personal mobile devices
- Share confidential information about the school, its children or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a child informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that children in my care do so too.

| | |
|---|---|
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 5: Mobile Phone Acceptable Use Agreement for Pupils and Permission

1. Pupils are not allowed to use mobile phones on school premises and if a pupil is found taking photographs or video footage with a mobile phone of either pupils or staff, this will be regarded as a serious offence and the pupils will be dealt with via the school's behaviour policy. If images of staff or pupils have been taken, the phone will not be returned to the pupils until the images have been removed in the presence of a senior teacher.

2. Pupils are not entitled to log on to the school network using their mobile phones or other personal electronic devices.

3. Mobile phones are to be kept in a tray in the classroom and are given back to pupils at the end of the day. Phones must be switched off (not just put on 'silent').

4. Pupils must avoid sharing their contact details with people they don't know, and must not share other people's contact details without their consent.

5. Pupils must not share their phone's passwords or access codes with anyone else.

6. When students enter the school grounds, the school takes no responsibility for mobile phones. Mobile phones are brought to school entirely at the owner's risk. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones.

7. Parents are reminded that in cases of emergency the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any appropriate way.

8. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device. The Headteacher will contact the parent to arrange the return of the phone. A repeat offence will lead to the child being refused permission to bring their phone to school.

PUPIL DETAILS

| | |
|---|---|
| Pupil Name: | |
| Pupil Class: | |
| Parent(s) name(s): | |

Pupils who bring a mobile phone to school must abide by the school's policy on the use of mobile phones, and its acceptable use agreement. The school reserves the right to revoke permission if pupils don't abide by the policy.

Parent signature: ________________________________________

Pupil signature: __________________________________________

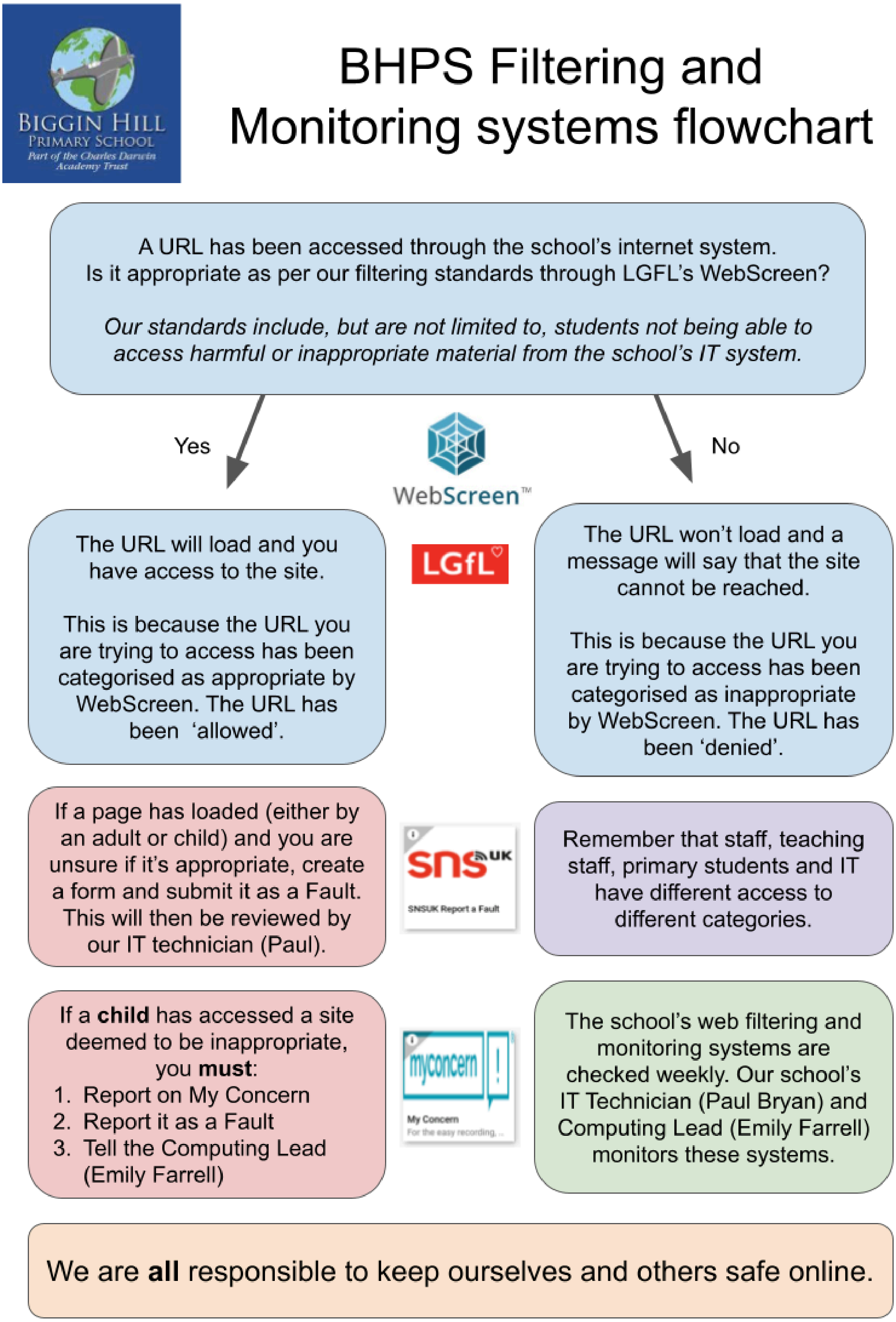
## Appendix 6: online safety training needs – self audit for staff

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Do you know what you must do if a child approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for children and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |
| Are you aware of the ways pupils can abuse their peers online | |

## Appendix 7: online safety incident report log

| 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** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Appendix 8: BHPS Filtering and Monitoring systems flowchart



# BHPS Filtering and Monitoring systems flowchart

A URL has been accessed through the school's internet system.
Is it appropriate as per our filtering standards through LGFL's WebScreen?

*Our standards include, but are not limited to, students not being able to access harmful or inappropriate material from the school's IT system.*

The URL will load and you have access to the site.

This is because the URL you are trying to access has been categorised as appropriate by WebScreen. The URL has been 'allowed'.

The URL won't load and a message will say that the site cannot be reached.

This is because the URL you are trying to access has been categorised as inappropriate by WebScreen. The URL has been 'denied'.

If a page has loaded (either by an adult or child) and you are unsure if it's appropriate, create a form and submit it as a Fault. This will then be reviewed by our IT technician (Paul).

Remember that staff, teaching staff, primary students and IT have different access to different categories.

If a **child** has accessed a site deemed to be inappropriate, you **must**:

1. Report on My Concern
2. Report it as a Fault
3. Tell the Computing Lead (Emily Farrell)

The school's web filtering and monitoring systems are checked weekly. Our school's IT Technician (Paul Bryan) and Computing Lead (Emily Farrell) monitors these systems.

We are **all** responsible to keep ourselves and others safe online.