



Document Owner	Sue Hornby	Governor ratification	Yes
Review period	Annually	Last reviewed	

## Pupil Online Policy

### 1. Introduction

#### The Six Principles

- 1.1 The BSM policy towards pupils online activity is based on these six principles
  - 1.1.1 Recognise that most of what young people do online is safe and there are many positives.
  - 1.1.2 Recognise that the Online World is the primary way most young people communicate outside school.
  - 1.1.3 Know that there will always be much we (adults) do not know.
  - 1.1.4 Accept pupils will often be the experts (and when they aren't they will believe they are)
  - 1.1.5 Build on the trust we have with our pupils and allow them to explain to us what they are doing.
  - 1.1.6 Be curious. (you will learn most from them both from a knowledge and safeguarding point of view if we listen to them and avoid 'lecturing')
- 1.2 Our overall aim is to enable pupils to engage in the online world in a way that is enriching, safe and respectful to others. We aim to support pupils to become inquisitive online users who are enabled to make informed choices about the integrity of the content that they are accessing.
- 1.3 Although the overall aim of this policy is to promote positive engagement with the online world, BSM is fully aware of the dangers of this environment. Section 3 of this policy expands in detail the safeguarding steps we will take. In brief our aims are for pupils to be aware of; -
  - 1.3.1 Their own safety & privacy.
  - 1.3.2 The safety & privacy of others.

- 1.3.3 That not everything they see online will be truthful and the intent of others users may not be what it appears.
- 1.3.4 What their digital imprint is saying about them and how it could be misinterpreted.
- 1.3.5 Their responsibilities to inform trusted adults of anything they are uncomfortable with or they believe could be of harm to themselves or others.
- 1.3.6 Their responsibility to engage with all aspects of online safety education provided by BSM.
- 1.3.7 How to act to safeguard themselves against these risks.
- 1.4 BSM will seek to enable pupils to safeguard themselves against all online risks.
- 1.5 This policy should be read in conjunction with the [Data Security & Safety Policy](#), if there is a contradiction between these please alert the policy owners of both policies.

### Definitions

- 1.6 In this policy these terms have these meanings
  - 1.6.1 'safety' refers to the safety of individuals from a safeguarding perspective, not the safety of data.
  - 1.6.2 'online' means any form of communication over a network including the internet, email, social media, SMS, phone call, local network (LAN).
  - 1.6.3 'staff' includes all employees of BSM, volunteers with pupil contact, and professional visitors to the school.
  - 1.6.4 'pupil' any young person attending any activity at BSM.

### Responsibilities

- 1.7 Responsibilities are as follows
  - 1.7.1 **SLT.** Overall responsibility for implementing this policy and ensuring other policies and practices are consistent with it, in particular those relating to safeguarding and conduct (staff and pupils). Hold the responsible managers to account. Actively seek advice from trusted sources (including external bodies).
  - 1.7.2 **Managers with IT responsibility.** Actively make themselves aware of changes and trends in the online world and in particular those concerning practices of young people and changes that could impact on pupil safety. Design internal courses that support pupils to achieve the aims of this policy. Report to SLT concern with any aspect of pupil online safety or teaching provision.
  - 1.7.3 **Staff.** Be aware and alert to trends and changes online and report concerns to management. Be a good role model to pupils and engage them in

dialogue about their online activity using the principles set out in the policy introduction.

- 1.7.4 Provide adequate supervision of pupils when accessing online material.
- 1.7.5 **Pupils.** Follow the guidance the school gives, inform trusted adults in the school of anything that concerns them. Be curious, and be safe.
- 1.8 Additional responsibilities specific to online safety are detailed in section 3 of this policy.

## **2. Teaching pupils about the online world**

- 2.1 The school will provide internal courses to deliver the intent of this policy in particular the six principles cited in the policy introduction.
- 2.2 Specific age appropriate programs will be developed for each of BSM three stages.
- 2.3 The content of the programs will be regularly reviewed taking into account
  - 2.3.1. Changes in the online environment.
  - 2.3.2. Changes in young people's use of the online world and in particular changes in use by pupils at BSM
  - 2.3.3. Current advice from respected agencies including National Online Safety campaign (NOS)
  - 2.3.4. Changes in legislation and official guidance.
- 2.4 It will be the primary responsibility of managers with IT responsibility to maintain internal courses to the best standards and up to date. However all staff have a responsibility to be alert to changes the school should take in all aspects of online activity including content of the courses taught.
- 2.5 Alongside the specific taught course good standards of online teaching will be embedded across all subjects. Teachers will take opportunities in all sessions to support pupils to use the online world positively and safely.

## **3. Online Safety**

- 3.1 Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are dangers related to their use, especially in relation to young people. Some examples of this are:
  - 3.1.1 Bullying via social media, including group chats
  - 3.1.2 Sexual and criminal exploitation, physical danger of sexual abuse
  - 3.1.3 Exposure to inappropriate materials and coercive 'fake news'
  - 3.1.4 Exposure to, and contact with, coercive or manipulative ideologies (including racism, misogyny, incel, transphobia, homophobia, terrorism and other ideologies identified in Prevent strategy)
  - 3.1.5 Other inappropriate or illegal behaviour
  - 3.1.6 Obsessive internet use

- 3.2 As a school it is our duty of care, alongside parents and carers, to protect children from these dangers. The Bridge will endeavour to ensure the online safety of all young people. It will use technology, education, accountability, responsibility and legislation as the key ways to achieve this. The school will also work closely with parents to ensure consistent messaging about online activity.

### Context

- 3.3 All young people are vulnerable to coercion of action and thought by people with extreme or dangerous views. The young people at BSM are typically more vulnerable due 'push' factors like 'identity', 'isolation', 'perceived injustice', 'victimisation', 'lacking sense of belonging' as well as 'pull' factors like 'social media', 'influencers', 'ideology' and especially 'seeking a sense of belonging'.
- 3.4 It is therefore imperative we are alert to these risks and are proactive in identifying and managing pupil online safety.

### School responsibilities for online safety

#### **3.5 Leadership and management responsibilities**

- 3.5.1 Ensure the school follows the latest RSE guidelines for delivering RSE and CEOPS in the curriculum.
- 3.5.2 Establish and maintain a system of 'filtering' to block content that is potentially risky to pupils, exposes them to offensive material or is inappropriate within a school.
- 3.5.3 Provide a system of 'monitoring' that allows the school to be alert to use of the school's online resources that might indicate dangerous or inappropriate use.
- 3.5.4 The balance between 'filter' and 'monitor' is to allow the pupils the maximum freedom to use the internet for their education and enjoyment while providing adequate safeguards against dangerous, offensive or otherwise inappropriate use.
- 3.5.5 Where appropriate, involve external agencies as part of investigations or for advice.
- 3.5.6 Brief new staff on the content of this policy and provide training as appropriate according to staff needs and the changing IT landscape.

CQ: Apart from initially, refresher for current staff?

#### **3.6 Staff Responsibilities**

- 3.6.1 Only use IT resources in school after a basic induction and signing the appropriate agreement in Section 3 of the [Data Security & Safety Policy](#)
- 3.6.2 Ensure pupils are not accessing material that impairs their learning by causing time wasting or is a distraction from learning.

3.6.3 Observe the the provision set-out in the Data Security & Safety Policy

### 3.7 Pupil responsibilities

3.7.1 Gaining an understanding of online safety issues and safe responses. Including actively engaging lessons specifically about online safety or other lessons where online safety is raised.

3.7.2 Compliance with Pupil's Acceptable Internet Use Agreement (appendix 1 of this policy) which pupils must agree to and sign at induction.

**GQ: Is this a once off or annual, biennial etc?**

3.7.3 Reporting any online safety issues to the coach or other staff immediately.

3.7.4 Take responsibility for their own actions using the internet and communications technologies.

### 3.8 Exceptions to this policy

The purpose of this policy is to protect pupils from improper or dangerous use of IT; not to restrict the use of IT in a way that limits pupil access to education or training. Therefore exceptions can be made when all of these conditions are met.

3.8.1 The pupil is in year 12 (or above) and engaged in vocational training or work experience.

3.8.2 A member of BSM staff has made an assessment of the use of IT and has concluded that restrictions around devices, filtering or unattended access would compromise the outcomes of the pupils' educational activity.

3.8.3 The activity has a specific risk assessment that makes reference to the exceptions to this policy.

3.8.4 Any exception to this policy is restricted only to the specific context of this activity.

### 3.9 Staff Infringements

Any infringement to the provisions of this policy will be a misconduct issues and will be managed in accordance with the Data Security and Safety Policy, and the Staff Disciplinary Policy.

## 4. Links to other policies and guidance

[Data Security and Safety Policy](#)

[Staff Disciplinary Policy](#)

[Child Protection and Safeguarding Policy](#)

Links to government guidance

[Revised Prevent duty guidance: for England and Wales](#)

[Police advice on CEOP](#)



# Appendix 1: Pupil's Acceptable Internet Use Agreement

## ***The internet is great...***

I can find out so much from the internet. It will help me find out a lot of good stuff to use in my education at the Bridge and beyond.

## ***But not everything on the internet is good...***

On the internet there is also a lot of material that is not nice. Some of it is unkind, hurtful or offensive. Some online content is inappropriate for my age or in a school.

## ***With the internet I can contact my friends...***

There are a lot of apps I can use to contact my friends. I can share ideas, memes, jokes, links to my favourite music or videos. We can talk about ourselves and our friends.

## ***But sometimes these apps are used incorrectly...***

These apps can be used to gossip, bully and tell hurtful lies. Sometimes things are said on these apps that we wouldn't say out loud and sometimes we write things that are misunderstood. It can be easy to hurt people without meaning to.

## ***Not everyone on the internet is my friend...***

There are people who use the internet to contact young people and try to get them to do things they wouldn't normally do. Often these people will seem friendly but they may mean to hurt me.

## ***I need to take control of my safety online...***

The most important person in protecting myself is me. If I think something is wrong on the internet (including my phone, computer, gaming platform, ipad etc) I need to tell an adult in school or at home. If something doesn't feel right I will tell someone.

## ***At the Bridge when using internet connected devices I will...***

- Find the best ways to use the internet for my education.
- Follow the instructions of my coaches.
- Tell a member of staff if I think I have found something not suitable for use in school or not appropriate for my age.
- Tell a member of staff if I am not comfortable with anything anyone has said online, even if it is from a friend.
- Tell a member of staff if I think another pupil has been bullied or hurt online.
- Not try to change any settings on any internet connected device (chromebook, computer, ipad etc)
- Not use my own devices in school unless clearly agreed with staff.
- Not use any device unless given permission by a member of staff
- Not try to get around the school internet filters or security features.
- Do my best to stay safe and help other pupils to be safe online.

I have read and understood the Bridge 'Pupil's Acceptable Internet Use Agreement'

Signed ..... Date .....

My Name ..... Coach present.....