BRIDGE HOUSE COLLEGE
IKOYI, LAGOS
....Knowledge for success

ONLINE SAFETY POLICY

Information & Communications Technology Department	**Approval Date:**	**Approved by:**
Policy: Online Safety Policy	**Date of next review:**	
Objective: to ensure the safety of students, staff and other stakeholders while using the internet and all other devices and tools used to access the internet		
Responsible Official:		
Responsible Advisory Board member:		
Signature:		
Data retention Policy Reference: • Acceptable ICT Use policy • Data Retention policy		

Application.

This policy has been authorised by the Advisory Board and is available to parents, students and staff on request.

1. Introduction

Bridge House College recognises that the internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** students, staff and board members will be supported to use the internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping our students navigate the online world safely and confidently.

2. Responsibilities

The Principal and board members have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this College is the IT Manager. All breaches of this policy must be reported to the Principal. All breaches of this policy that may have put a student at risk must also be reported to the Designated Safeguarding Lead, Bridge House College.

3. Scope of policy

The policy applies to:

- Students
- parents/house parents
- teaching and support staff
- the leadership team
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors

The College also works with partners and other providers to ensure that students who take part in online lessons or who are on a College trip are safe online.

The College provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their children to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole College community. It is linked to the following other College policies and documents: Safeguarding, Acceptable ICT Use, Data Retention and anti-bullying policies.

4. Policy and procedure

The College seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The College expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of College for students, parents/carers, staff and governors and all other visitors to the College.

Use of email

Staff and management team should use a College email account for all official College communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any College business using a personal email address. Students should use College approved accounts on the College system for educational purposes. Where required, parent/carer permission will be obtained for the student account to exist.

Staff, management team and students should not open emails or attachments from suspect sources and should report such emails to the IT Manager.

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

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in College or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content.

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

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult materials

- Promoting discrimination of any kind in relation to the protected characteristics: age, gender, disability, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief.

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the College or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the College

- Use the College's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others

- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the College

Only a College device may be used to conduct College business outside of College. The only exception would be where a closed, monitorable system has been set up by the College for use on a personal device. Such a system would ensure the user does not save files locally to their own device and breach data security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

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

Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the College. In line with General Data Protection Regulation they are used only with the written consent of parents/carers which is secured in the first instance on a student's entry to the College. Records are kept on file and consent can be changed by parents/carers at any time.

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

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

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

Use of personal mobile devices (including phones)

The College allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas.

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

Students are allowed to bring personal mobile devices/phones (without camera and internet capacities) to College but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off. Under no circumstance should students use their personal mobile devices/phones to take images of

- any other student unless they and their parents have given agreement in advance
- any member of staff

The College is not responsible for the loss, damage or theft of any personal mobile device that is brought into College.

Users bringing personal devices into College must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access College emails and data. The only exception would be where a closed, monitorable system has been set up by the College for use on a personal device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the College must consider educational benefit and carry out risk assessment before use in College is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in College and should check with the Principal before they are brought into College.

Reporting incidents, abuse and inappropriate material

There may be occasions in College when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSL, the ADSL or the Principal. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The College takes the reporting of such incidents seriously and where judged necessary, the DGS will refer details to the police.

5. Curriculum

Online safety is fully embedded within our curriculum. The College provides a comprehensive age appropriate curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

6. Staff and Management Team Training

Staff and management team are trained to fulfil their roles in online safety. The College audits the training needs of all College staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the College's Acceptable Use Agreement as part of their induction and before having contact with students.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement

Guidance is provided for occasional visitors, volunteers and parent/carer helpers

7. Working in Partnership with Parents/Carers

The College works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and College. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.
It is important that parents/carers understand the crucial role they play in this process. The College seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The College provides regular updated online safety information through the College website, newsletters and by other means.

8. Records, monitoring and review

The College recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to students and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported

The College supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt according to sanctions laid down in the Student Handbook. Breaches may also lead to criminal or civil proceedings.

The DGS receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, the DGS should ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.