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

BRIDGE HOUSE COLLEGE
...Knowledge for success

ONLINE SAFETY POLICY

Information & Communications Technology Department	**Date Reviewed: June 2024**	**Date Approved :** 04/02/2025
Policy: Online Safety Policy	**Date For Next Review: June 2025**	**Approved by:** Kamal Abdulkarim
Objective: To ensure safety of students, staff and the management team while using the internet and all other tools available on the internet		
Responsible Official:		
Responsible Office:		
Signature:		
Data retention Policy Reference: General Data Protection Regulation 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 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 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 children and young people 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 school is Mr. Adebayo.
All breaches of this policy must be reported to the Principal.
All breaches of this policy that may have put a child 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
- school management team
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school 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 school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, General Data Protection Regulation, health and safety, home–school agreement, home learning, behaviour, and anti-bullying policies.

4. Policy and procedure

The school 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 school 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 school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and management team should use a school email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address. Students should use school approved accounts on the school 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 their receipt to Mr Adebayo.

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 school 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, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex.

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

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

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

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 school

- Use the school'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 school

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

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

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the 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 school. 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 school. 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 school'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 pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

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

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

Use of personal mobile devices (including phones)

The school 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 school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Principal. When a parent/carer is on school 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 school 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 school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

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

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

New technological devices

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

Reporting incidents, abuse and inappropriate material

There may be occasions in school 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 school 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 school 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 school audits the training needs of all school 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 school'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 school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. 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 school 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 school provides regular updated online safety information through the school website, newsletters and by other means.

8. Records, monitoring and review

The school 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 pupils 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 school 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 with under the school's behaviour and disciplinary policies as appropriate. 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, governor 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.

Online Safety Acceptable Use Agreement - Staff

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

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

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Mr Adebayo.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, the Principal and others as required.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or students

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in acceptable ICT use and Data retention policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the Principal or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, students or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address for all school business. All such correspondence must be kept professional. I will not use my school email addresses for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Principal.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Mr Adebayo.

Promoting online safety

I understand that online safety is the responsibility of all staff and board members and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, board members, visitors, students or parents/carers) to the DSL or the ADSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of students. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Principal.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership. Principal and DSL. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment.

Signature ..... Date .....

Full Name .....

Job title .....

Online Safety Acceptable Use Agreement Students

- I will only use school IT equipment for school purposes.
- I will not download or install software on school IT equipment.
- I will only log on to the school network, other school systems and resources using my own school user name and password.
- I will not reveal my passwords to anyone other than a parent/carer.
- I will not use my personal email address or other personal accounts on school IT equipment.
- I will make sure that all my electronic communications are responsible and sensible.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff if I am in school, or parent/carer if I am not in school.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- I should never post photographs, videos or livestream without the permission of all parties involved.
- I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
- I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
- I will not attempt to bypass the internet filtering system in school.
- I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
- I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that students are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Pupils are expected to read and discuss this agreement with you and then sign below to show they will follow the terms of the agreement. Any concerns or explanation can be discussed with the DSL.

Please can you also sign and return the parent/carer agreement below.

This document will be kept on record at the school.

Student agreement

Student name.....

I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Student signature.....

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s).....

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

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

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

Parent(s)/carer(s) signature(s) .....

Date .....