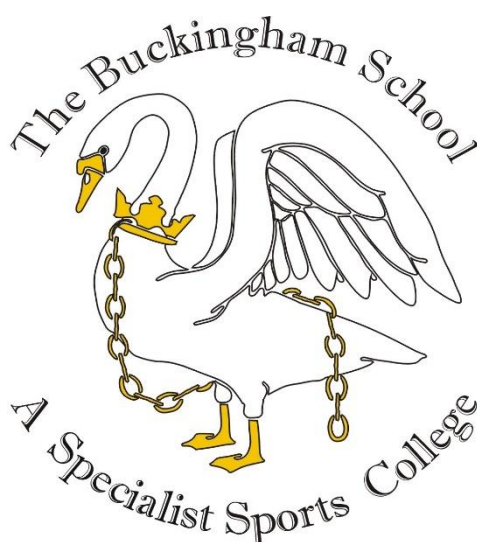


**E SAFETY / ONLINE POLICY  
FOR  
THE BUCKINGHAM SCHOOL**



**NAMED PERSON: DAVID OSBORNE**  
**ATTACHED COMMITTEE: PERFORMANCE**

**REVIEWED: APRIL 2020**  
**REVIEW CYCLE: 1 YEAR**  
**NEXT REVIEW DATE: APRIL 2021**

## **Aim of the Policy:**

This policy outlines and clarifies what is expected by staff at The Buckingham School, responsibilities in educating students and guidance on safe guarding themselves online.

## **Responsibility and education:**

Parental awareness and personal setup of Online / E-Safety is the responsibility of Designated Safeguarding Lead (DSL), under the guidance of the Headteacher.

Parent and student education of the benefits, risks and responsibilities of using *information technology* is through Assembly Messages, Safer Internet Assemblies, Parental Awareness Evenings, PHSE Lessons, Personal Development and Enrichment Days. Staff, student and parent education is supplemented by School Police Liaison Officers input. Parents are able to attend an Online / E-Safety evening organised on a biennial basis at TBS/RLS to raise the awareness of on-line safety. Further links to CEOP/ Think You Know organisations and further reading are available for staff education.

## **Expectations of Staff:**

### **Use of internet**

Staff are to use the internet to extend and enrich learning. Staff are to educate students in what constitutes copyright infringement, plagiarism of information, and ensure students are aware of how to reference online sources.

### **Sites**

The school's internet filtering is designed expressly for student use allowing access to pre-defined categorised lists of sites. Staff are responsible for reporting any sites that require blacklisting.

The school uses keyword detection software that flags words from extensive set of libraries including adult content, bullying and trolling, counter-radicalisation, drugs and substance misuse, eating disorders, grooming, illegal content, LGBT derogatory language, race and religious hatred, sexual assault, self-harm, sexting, suicide and weapons and violence. Words written in applications, emails and browsers generate an alert for all stakeholders. Students are contacted within 12 hours of alert generation, with the aim to contact each student within an hour of the alert.

The school will take precautions to ensure that users access only appropriate material however, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed or any consequences resulting from Internet use.

## **Student Use of social Media**

What is and isn't acceptable is outlined in the student IT Acceptable Use Policy (AUP). In registering to attend our school, students agree to abide by the IT Acceptable Use Policy. The school's duty of care extends beyond the school. Social networking sites are not accessible on the school network but acknowledges that students will make use of them outside of school. When the impact of a particular online behaviour is felt in school, and/or when, the wellbeing of members of the school community is compromised and school will act and investigate as part of its duty of care.

Students are to be educated in the potential repercussions of what they post. Details that identify them or their location should never be shared online. Students are to be educated not to post personal photos on any social network space, including the background details in a photograph which could identify the student or his/her location.

Staff should report student breach of IT Acceptable Use Policy. Minor transgressions of the IT Acceptable Use Policy may be dealt with routinely by the class teacher; however more serious incidents will be dealt with in conjunction with the Behaviour for Learning Policy and Safeguarding Policies. Potential child protection issues are referred to the DSL immediately.

Pictures of students published on the web:

Publication consent will be sought from parents at the time the student joins the school, staff must be vigilant when taking any photos that student consent has been given. Images of students must not be used where consent has not been provided. Staff must ensure that all pictures of students taken, must be appropriately clothed, and students must never be named.

**Success for All through Achievement, Challenge & Enjoyment**

---

## Staff use of social media

The open nature of the internet and social networking means that everyone should take active steps to protect themselves by taking some simple precautions. Staff must safeguard themselves to avoid compromising their professional position.

### Protect professional reputation

Professional reputation is an essential part of staff's current and future career. Managing online reputation is essential. Staff are advised to think carefully before posting information online about their school/college, staff, students or parents even if your account is private.

Comments that are made public could be taken out of context and could be very damaging. The language used is important, as abrupt or inappropriate posts may lead to complaints. Anything that posted online is potentially public and permanent.

Staff are advised to think carefully as to how they present themselves, when they post images or when joining a group or 'liking' pages. Choices will say something about you. An employer may reasonably believe that a recognisable member of staff putting an inappropriate post or image in the public domain will lower the reputation of the school or college. This could be a basis for disciplinary action. It is an implicit condition of employment that an employee owes a duty of loyalty to an employer.

### Choose your friends carefully

Staff are to consider carefully whom they are friends with online and which friends can access what information. Unions and TBS strongly advises that staff do not accept friend requests, or requests to follow, on personal accounts from students, past or present or from parents at the school. By accepting such requests, staff could be making themselves vulnerable by sharing personal information or by having access to personal information about students. This could leave staff open to allegations of inappropriate contact or conduct and they could find yourself exposed to unwanted contact.

### Privacy settings

It is important that when using social networking websites staff are in control of who can see their account details and content including photos and albums, posts, status updates and any personal information.

#### Privacy settings across all social media platforms:

Please ensure it is not only Facebook your privacy settings are robust, both Instagram and SnapChat are high profile and frequently used platforms and staff must protect themselves appropriately from images and messages published on these forums. Students regularly attempt to connect with staff and with robust privacy settings these requests will be filtered out.

Setting to 'Friends only' will enable staff to achieve a good degree of privacy. It is strongly suggested that staff customise each option further and limit the information that certain people can see. Staff profile picture is public on Facebook and there is no way to make it private and by default all past profile pictures are public unless manually set to private.

If staff are not entirely sure about how to use all the settings, Facebook has a privacy check that will guide staff through how to maximize the privacy settings. It is a good idea to remove any friends, or customise the privacy settings for current friends, if access to personal activity, could compromise your position. It is important, regardless of which setting staff use, that staff think about what they post because 'friends' settings do not guarantee privacy.

Staff are advised to be careful about comments posted on your friends' walls and shared posts because if their profile is not set to private, staff posts will be visible to everyone. Sharing content with others could mean that staff lose control of it; for example, friends could pass on staff information.

Staff use of robust security settings on social networking accounts will protect staff from information breaches. If confidential information that should have remained within the organisation has been revealed on staff accounts, the fact that the leak has been exposed by a criminal is irrelevant. Staff username and password are their property and therefore staff are responsible for them. If someone has access to them and posts something on that staff account, the staff member is indirectly responsible for the information being posted.

## Staff should be aware and manage what others post about them online

Staff are encouraged to search their name regularly online to monitor any content about themselves. This enables staff to see what others can and provides an opportunity for staff to remove or ask friends to un-share anything that may compromise your reputation. Other people could post images on their profile in which staff are named, so think about any photos that staff members appear in. On Facebook, staff are encouraged to 'untag' themselves from photos. If staff do find inappropriate references to themselves and/or images of posted by a friend online, staff should contact them and ask that the content be removed. Alternatively, staff could go directly to Facebook to request that the photos be taken down.

## Reporting concerns

Concerns over staff misuse that may constitute a breach of policy and /or bring the school into disrepute must be reported to the Head of Computing/ IT Support Team. The school may exercise its right by electronic means to monitor the use of the school's computer systems (See TBS IT AUP) where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful under GDPR.

## Online harassment

There is a duty of care on the part of the LEA to protect staff from harassment. If the LEA fails in this duty and staff suffer harm, they could be legally liable. Staff are to contact the service provider to have the offending remarks deleted or website closed down. If this is not successful, The Buckingham School would consider it appropriate to take legal action (or make use of the employer's legal advisers for example, the LA or retained lawyers) to tackle the issue both because the employer should be protecting its employees from harassment and because such a slur on an employee is also a slur on the employer.

Another possibility is to approach the police. If the comments are offensive enough and frequent enough it might mean that they can be counted as harassment in the criminal sense. It is difficult to make a legal case for defamation. For a statement to be defamatory, it must tend to lower the claimant in the estimation of right-thinking members of society generally. A statement that amounts to an insult or is mere vulgar abuse is not defamatory. This is because the words do not convey a defamatory meaning to those who heard them (simple abuse is unlikely to cause real damage to a reputation).

*I have read and fully understood the Online / E-Safety policy above and will adhere to these policies and the above rules.*

Please sign the below to confirm:

Staff Member Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Full Name: \_\_\_\_\_


THE BUCKINGHAM SCHOOL – A SPECIALIST SPORTS COLLEGE



## Online / E-Safety Policy

REVUEWED: APRIL 2020  
NEXT REVIEW: APRIL 2021

Mr Matthew Watkins  
Chairman  
Governing Body

Signed: 

Date: April 2020