Westbourne School

Westbourne Road, Sheffield, S10 2QT (Tel: 0114 266 0374)

School use of Social Media Policy

Person Responsible	Online safety coordinator - Miss Katie Baker
Date Written	Sept 2021
Review Date	Sept 2022

Contents

1. Scope

This policy specifically covers the use of social media accounts set up in the school's name. Any social media account set up in the name of the school is covered by, and must adhere to this policy.
Social media use is mentioned in several other policies, in most circumstances other policies cover the personal use of social media.

Social Media in other policies.

- Acceptable Use Policy
- Data Protection Policy and GDPR notice
- Online Safety Policy
- Safeguarding Children Policy
- The Staff Handbook section on social media

For the purpose of this policy an image is defined as any content, digital or otherwise, that shows a visual representation of a person, this definition includes, but is not limited to, photographs and video recordings.

2. Objectives

To ensure that the personal data of all staff and students are kept safe.
To ensure that school social media is used responsibly.
To ensure that the school adheres to all legislative guidance.

3. Why a policy is required

Social media can be an excellent marketing tool and it can be a great way to celebrate the achievements of the school and it's students. However, everyone involved needs to be aware that placing any identifying information in the public domain has risks. Parents also need to understand these risks in order to give properly considered consent.

The most highly publicised and worrying risk is that a child who appears on social media may become of interest to a predatory sex offender. Locating people through the internet has become extremely easy, using widely available software, so if there is a picture and the name of the school and the name of a child it could be quite easy to find out the address of the child and even work out their most likely route to school.

There are also other specific groups of children and families whose safety could be put at risk if identified, e.g. looked after children.

Any image or other personal information, once posted online, can be copied or shared by anyone and will stay online forever. There is also the concern that images of children may be copied directly from social media and then manipulated or changed by another person.

To limit these potential risks the school must take appropriate steps to safeguard children.

4. Roles and Responsibilities

The Headteacher, Designated Safeguarding Lead (DSL) and Online Safety Coordinator will be responsible for the implementation of this policy.

The Online Safety Coordinator will ensure this policy is kept up to date and that staff using school social media have the necessary training.

The Director of Marketing and Admissions will have access to any and all social media accounts set up in the schools name and will ensure the content posted adheres to this policy.

The Data Protection Officer is responsible for ensuring the acceptable and safe storage of all images within the school.

Any member of staff who takes images or records videos for social media use and any staff who has access to post or add content of any kind to a social media account set up in the name of the school should read, understand and follow the guidelines set out in this policy.

Any breach of this policy may result in disciplinary action. Any member of staff suspected of breaching this policy will be required to cooperate with an investigation, which may involve accessing relevant passwords and login details. This would be in accordance with an employee's legal rights.

This policy is not intended to restrict all employee activity on social media. However, school representatives are asked to exercise caution and professional judgement about what they use it for, who they communicate with and the subject matter they post and interact with.

5. Official use of Images / Videos of Children by the School

5.1 Taking Images

Staff should use school devices to take pictures. Staff should ensure that when taking images, only students with consent should be in the image. Staff should ensure that pupils are aware when images are being taken of them, this is for the safety of the pupils and the staff taking the images. For clarification of consent, see section 5.4 of this policy.
Care should be taken when taking images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

At school events such as school music and theatre productions, sports day, school prom and school discos, images should only be taken by members of staff selected to be the official photographers. Other staff members, volunteers or temporary staff members helping to run an event should not take photos or videos.
EYFS staff should be aware that ISI have stated that use of mobile phones and cameras in EYFS settings should be restricted (see Appendix A of Safeguarding and Child Protection Policy). This is also covered in the school's safeguarding policy.
Any staff taking pictures of pupils with their own personal device must install the 'Google Apps Device Policy' on their mobile device. When using a personal device staff must always use the school camera app called Open Camera. This gives the school the ability to wipe any school data from the device should it be misplaced, it also prevents school photos being saved to personal accounts. Any staff who use a personal device to access school storage should ensure that they have read and understood the Online Safety Policy Section that covers staff use of personal devices. Any images accidentally taken using a personal camera app must be deleted immediately / as soon as the staff member becomes aware of the mistake. Steps should be taken to ensure the images have not been backed up onto personal cloud storage automatically, and should be deleted immediately if this has happened.

5.2 Storage of Images

All images taken by the school will be stored in a safe and responsible manner that adheres to data protection principles.
Any staff who use a personal device to access school storage should ensure that they have read and understood the Online Safety Policy section that covers staff use of personal devices.
Once a student has left the school their image should not be used on social media unless the former student is contacted (or the former student's parents if the former student is still a child) and written consent is given.

5.3 Posting Content on Social Media

All staff must be aware that when content, including images, is uploaded to social media then the user agrees to the terms and conditions of that social media. For many social media websites this would mean that by uploading any images or videos the school is granting the site a license to copy, modify and use the images. This means that the school no longer "owns" the content and it can be used without the school's consent or knowledge. To adhere to GDPR the Data Controller should undertake a risk assessment on any

website or app that is used to share content, to identify possible dangers and what actions may be taken by the school to limit any concerns.
The school should keep track of who has access to public facing social media accounts set up in the school's name, everyone who has access should receive adequate training on the safe and responsible use of social media. Public facing social media accounts will be managed by the Director of Marketing and Admissions and two Social Media Managers, one in Junior School and one in Senior School.
Through their school Google account all staff will have access to Google Currents, although this is a form of social media, it has been set so that posts are not publicly shared. They are only accessible to staff with a Westbourne Google account. Despite this, staff would ensure they use Google Currents with the same professionalism that they do all other school communications. Students will not have access to Google Currents via their school Google account.

Specific guidance on social media posts:

- Any social media post created by an account that has been set up in the school's name should include as few personal details as possible.
- For every post staff should consider whether it is really necessary to include the chosen level of detail; could detail be minimised further.
- The full name (first name and surname) of a child or adult should never be used in a post that contains an image.
- If the full name (first name and surname) of a child or adult must be used, then it must be done so without an image.
- If a photograph is of an individual child then that child's first name should not be used.
- If a child has left the school their personal details, including images, should not be used in any new social media post, unless the school has gained written consent to continue using them.
- Personal contact details such as email, postal address and telephone numbers should not be used in any post at any time.
- If the school has a specific reason for breaching any of these guidelines in a specific post, they should ask for specific written consent to do so for that post only. Consent should come from parents if the child is under 12. If the child is 12 or over consent should come from parents and the child in question.

5.4 Consent

An image of a person is considered personal data and it is a requirement that written consent is obtained from the parent / carer of a young child or young person under the age of 12 (or from him or herself if deemed to be competent to make such judgements from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings.
The school will get general consent for the use of images when students join the school. Parents / carers will be made aware, prior to giving consent for images to be taken, that their child's image may be posted on social media.
Verbal consent must not be accepted under any circumstances. If it is not possible to obtain prior written consent, then images must not be taken involving the child or young person concerned.
The parent / carer has the right to refuse or withdraw consent at any time. Any images of a child whose parents have refused or withdrawn consent, must be destroyed.

If two parents disagree over consent for their child to appear in images, the school should treat this as though no consent has been given.
Consent should also be obtained from any staff member who appears in an image to be posted on social media.

5.5 Contact with students on social media

Communication between children and adults should remain professional at all times.
The school should never use school social media accounts to add or follow students.
The school should never build or pursue relationships with children online, even if the child has left the school.
The school should never use the private messaging services linked to social media accounts to contact any staff, student, parent or family member of a student. Contacting anyone digitally should always be done through official channels, such as official school email accounts.
If a request is received from a child to add or follow school social media accounts this may be accepted. All children should be educated on the risks of social media, for more on this see the school Online safety Policy.
Staff who have access to school social media accounts should ensure that all communications are transparent and open to scrutiny.

5.6 Use of images of Children by the Press

Occasionally images and personal details of students may be released to the press. It should be noted that the press enjoy special rights under the Data Protection Act, which permit them to publish material for journalistic purposes. In every case consent should be requested from parents before releasing any personal details to the press. Where students are over 12 years of age the student should also be asked to give consent for their personal details to be given to the press.

5.7 Liking, sharing and retweeting.

Staff should ensure that any post created by any other account that is linked to the school social media account via liking, sharing, retweeting or any other method that allows direct connection between the school and that post, is also inline with this policy. Staff using the school social media account should not like, share or retweet any post from any other account if it contains too many personal details about students or staff. For guidelines about what constitutes too much personal detail see the guidelines in section 5.3.

6. Raising Concerns

If any member of staff has a concern about any post or content on any of the school social media accounts they should raise it with the Director of Marketing and Admissions, the Online Safety Coordinator and/or the Safeguarding Lead.
If a child or parent makes a complaint to you please forward this to the Director of Marketing and Admissions, the Online Safety Coordinator and/or the Safeguarding Lead.