**PERRYFIELDS PRIMARY PRU**

****

**SOCIAL MEDIA POLICY**

**April 2020**

|  |  |  |  |
| --- | --- | --- | --- |
| **Review Date** | **Reviewed Date** | **Reviewer (Who?)** | **Action** **(Ratified by Management Committee - Who?)** |
| **March 2022** |  |  | **Ratified by Management Committee** |
|  |  |  |  |
|  |  |  |  |

**Statement of intent**

Perryfields Primary PRU understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

* Encouraging the responsible use of social media by all staff, parents and pupils in support of the school’s mission, values and objectives.
* Protecting our pupils from the dangers of social media.
* Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
* Protecting our staff from cyber bullying and potentially career damaging behaviour.
* Arranging e-safety meetings for parents

**Legal framework**

This policy has due regard to legislation and guidance including, but not limited to, the following:

The General Data Protection Regulation (GDPR)

DfE (2018) ‘Data protection: a tool kit for schools’

The Data Protection Act 2018

This policy will be implemented in accordance with the following school policies and documents:

Acceptable Use and E-Safety Agreement

E-Safety Policy

Data and E-Security Breach Prevention and Management Plan

Data Protection Policy

Complaints Procedures Policy

Anti-Bullying Policy

Allegations of Abuse Against Staff Policy

Photos and Videos Policy

**Roles and responsibilities**

The headteacher is responsible for:

The overall implementation of this policy and ensuring that all staff, parents and pupils are aware of their responsibilities in relation to social media use.

Promoting safer working practices and standards with regards to the use of social media.

Establishing clear expectations of behaviour for social media use.

Ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.

In conjunction with the Management Committee, handling complaints regarding this policy and its provisions in line with the school’s Complaints Policy.

Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.

Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.

Working alongside the e-safety officer and data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with the GDPR.

Staff members are responsible for:

Adhering to the principles outlined in this policy and the Acceptable Use and E-Safety Agreement.

Ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.

Reporting any social media misuse by staff, pupils or parents to the headteacher immediately.

Attending any training on social media use offered by the school.

Parents are responsible for:

Adhering to the principles outlined in this policy

Taking appropriate responsibility for their use of social media and the influence on their children at home.

Promoting safe social media behaviour for both themselves and their children.

Attending e-safety meetings held by the school wherever possible.

Pupils are responsible for:

Adhering to the principles outlined in this policy

Ensuring they learn how to use social media appropriately and stay safe online.

**Definitions**

For the purpose of this policy, the school defines **“social media”** as any online platform that offers real-time interaction between the user and other individuals or groups.

For the purpose of this policy, **“cyber bullying”** is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.

For the purpose of this policy, **“members of the school community”** are defined as any teacher, member of support staff, pupil, parent of a pupil, governor or ex-pupil.

**Data protection principles**

The school will obtain consent from pupils and parents at the beginning of each academic year using the Images and Videos Parental Consent Form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the entire academic year.

A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The DPO is responsible for ensuring this consent record remains up-to-date.

Parents and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the school in writing.

Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents’ and pupils’ requirements following this.

The school will only post images and videos of pupils for whom consent has been received.

Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the headteacher for use.

The school will not post pupils’ personal details on social media platforms.

Pupils’ full names will never be used alongside any videos or images in which they are present.

Only appropriate images and videos of pupils will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.

When posting on social media, the school will use group or class images or videos with general labels, e.g. ‘sports day’.

Before posting on social media, staff will:

* Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
* Ensure that there is no additional identifying information relating to a pupil.

Any breaches of the data protection principles will be handled in accordance with the school’s Data and E-Security Breach Prevention and Management Plan.

Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.

Social media use – staff

School accounts

Staff will not post any content online which is damaging to the school or any of its staff or pupils.

If inappropriate content is accessed online, a [report form](#BB) will be completed and passed on to the e-safety officer. The e-safety officer retains the right to monitor staff members’ internet usage in line with the Data and E-Security Breach Prevention and Management Plan.

Personal accounts

Staff members will not access social media platforms during lesson times.

Staff are not permitted to use the school’s WiFi network to access personal accounts, unless otherwise permitted by the headteacher, and once the e-safety officer has ensured the necessary network security controls are applied.

Staff will not use social media in front of pupils.

Staff will not “friend” or otherwise contact pupils or parents through their personal social media accounts.

If pupils or parents attempt to “friend” a staff member they will report this to the headteacher.

Any contact with pupils or parents will be done through authorised school contact channels.

Staff members will ensure the necessary privacy controls are applied to personal accounts.

Staff members will avoid identifying themselves as an employee of Perryfields Primary PRU on their personal social media accounts.

No staff member will post any content online that is damaging to the school or any of its staff or pupils.

Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of Perryfields Primary PRU.

Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.

Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.

Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.

Members of staff will regularly check their online presence for negative content via search engines.

Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

Members of staff will not leave a computer or other device logged in when away from their desk or save passwords.

Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

**Social media use – pupils and parents**

Pupils will not access social media during lesson time, unless it is part of a curriculum activity.

Pupils and parents will not attempt to “friend” or otherwise contact members of staff through their personal social media accounts. Pupils and parents are only permitted to be affiliates of school social media accounts.

Where a pupil or parent attempts to “friend” a staff member on their personal account, it will be reported to the headteacher.

Pupils and parents must not post anonymously or under an alias to evade the guidance given in this policy.

Pupils and parents must not post any content online which is damaging to the school or any of its staff or pupils.

Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil’s age.

If inappropriate content is accessed online on school premises, it will be reported to a teacher.

Pupils are not permitted to use the school’s WiFi network to access any social media platforms unless prior permission has been sought from the headteacher, and the e-safety officer has ensured appropriate network security measures are applied.

**Blocked content**

In accordance with the school’s Data and E-Security Breach Prevention and Management Plan, the e-safety officer installs firewalls on the school’s network to prevent access to certain websites. The following social media websites are not accessible on the school’s network:

* Twitter
* Facebook
* Instagram

Attempts made to circumvent the network’s firewalls will result in a ban from using school computing equipment, other than with close supervision.

Inappropriate content accessed on the school’s computers will be reported to the e-safety officer so that the site can be blocked.

The e-safety officer retains the right to monitor staff and pupil access to websites when using the school’s network and on school-owned devices.

Requests may be made to access erroneously blocked content by submitting a [blocked content access form](#AA) to the e-safety officer, which will be approved by the headteacher.

**Cyber bullying**

**See Cyber bullying policy**