



# Damers First School

## Social Media Policy

Date policy last reviewed: September 2023

Signed by:

\_\_\_\_\_ Head of School      Date: \_\_\_\_\_

\_\_\_\_\_ Chair of governors      Date: \_\_\_\_\_



## **Contents:**

### Statement of intent

1. Legal framework
2. Roles and responsibilities
1. Definitions
2. Data protection principles
3. Staff social media use
4. Parent social media use
5. Pupil social media use
6. Online safety
7. Blocked content
8. Cyberbullying
9. Training
10. Monitoring and review

### **Appendices**

- A. Photography and Video at Damers form

## **Statement of intent**

Damers First School 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, carers 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 cyberbullying and potentially career damaging behaviour.
- Arranging online safety information for parents and carers.

## 1. Legal framework

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

- DfE (2018) 'Data protection: a toolkit for schools'
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Freedom of Information Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- DfE (2023) 'Keeping children safe in education 2023'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Anti-Bullying Policy
- Safeguarding and Child Protection Policy
- Staff Disciplinary Policy
- Technology Acceptable Use Agreement
- Staff ICT and electronic Devices Policy
- Staff Code of Conduct
- Password Policy
- Complaints procedure

## 2. Roles and responsibilities

The Head of School 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 against any of the protected characteristics, as outlined in the Equality Act 2010.
- In conjunction with the governing board, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedures 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 online safety officer and data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with UK GDPR.

The governing board is responsible for:

- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.

- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

Staff members are responsible for:

- Adhering to the principles outlined in this policy and the Technology Acceptable Use Agreement for Staff.
- 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 Head of School immediately.
- Attending any training on social media use offered by the school.
- Handling inappropriate comments or abuse posted on the school's social media accounts, or regarding the school if required by the Head of School.

Parents are responsible for:

- Adhering to the principles outlined in this policy and the Social Media Code of Conduct for Parents.
- 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 online safety meetings held by the school if or when arranged.
- Not engaging in activities involving social media which might bring the school into disrepute.
- Not representing their personal views as those of the school on any social medium.
- Acting in the best interests of pupils when creating, participating in or contributing to social media sites.

Pupils are responsible for:

- Adhering to the principles outlined in this policy
- Ensuring they understand how to use social media appropriately and stay safe online.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Demonstrating the same high standards of behaviour as expected within the school.

The ICT Technician is responsible for:

- Monitoring and reviewing any school-run social media accounts.
- Vetting and approving individuals who wish to be 'friends' or 'followers' on the school's social media platforms.
- Consulting with staff on the purpose of the social media account and the content published.
- Maintaining a log of inappropriate comments or abuse relating to the school if required by the Head of School.

- Handling inappropriate comments or abuse posted on the school's social media accounts, or regarding the school if required by the Head of School.
- Ensuring that enough resources are provided to keep the content of the social media accounts up-to-date and relevant.
- Providing technical support in the development and implementation of any of the school's social media accounts.
- Implementing appropriate security measures as directed by the Head of School.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

### 3. 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 including, but not limited to, the following:

- Blogs
- Online discussion forums, such as NetMums
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- ‘Micro-blogging’ applications, such as Twitter

For the purpose of this policy, “**cyberbullying**” 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.

### 4. Data protection principles

The school will obtain consent from pupils and parents at the beginning of each academic year using the Photography/Video Consent Form (appendix 1), 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. 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. Consent is obtained from whoever holds parental responsibility for the pupil.

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 and can do so by contacting the school office. 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.

Consent can be provided for certain principles only, for example only images of a pupil are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided. 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 ICT Technician for use. 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'.

To reduce the risk of a pupil being identified, the school will not post pupils' personal details on social media platforms and pupils' full names will never be used alongside any videos or images in which they are present.

Before posting on social media, staff will:

- Refer to the consent management database 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 Protection Policy and Cyber Response Plan.

## **5. Staff social media use**

### **School accounts**

The school's social media sites will only be created and monitored by the ICT Technician and other designated staff members. There will be a strong pedagogical or business reason for the creation of social media accounts on behalf of the school; official school profiles and accounts will not be created for trivial reasons.

If members of staff wish to create a new social media account, they will seek the approval of the Head of School. The ICT Technician will then create the account on the behalf of the requesting individuals and support them in its management.

A school social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official school email account.

Consideration will be given to the following aspects:

- The purpose for using social media
- Whether the overall investment will achieve the pedagogical aim
- The level of interactive engagement with the site
- Whether pupils, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the proposed site
- A clear plan which outlines aspects such as how long the site will last



- How the success of the site will be evaluated

School social media passwords are kept by the relevant member of staff responsible for the account on the particular social media platform and the ICT Technician. These are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the Head of School. Staff will adhere to the data protection principles outlined in [section 4](#) of this policy at all times, and refer to the Data Protection and Password policies.

Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the school or any achievements. Staff will not post any content online which is damaging to the school or any of its staff or pupils.

All content expressed on school social media accounts will not breach copyright, data protection or freedom of information legislation.

The school's social media accounts will comply with site rules at all times. It will be noted that each networking site has their own rules which must be followed – the ICT Technician will induct staff to each new social media platform, providing them with the relevant training and information.

### **Personal accounts**

Staff members will not access social media platforms during lesson times, but they are permitted to use social media during break times. Staff will avoid using social media and any personal devices in front of pupils.

Staff members will not use any school-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught. Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the Head of School, and once the ICT Technician has ensured the necessary network security controls are applied.

Staff will not 'friend', 'follow' or otherwise contact current pupils through their personal social media accounts. If pupils attempt to 'friend' or 'follow' a staff member, they will report this to the Head of School.

Staff must be cautious about following or being followed by parents/carers of pupils, accepting parents of pupils as friends on Facebook or having contact with parents/carers on any social networking site. Adults must be mindful at all times of the boundaries between their work and personal life.

Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels. 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.

Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the school on their personal social media accounts. Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not those of the school.

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

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.

Social media will not be used as a platform to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals.

Staff members' personal information will not be discussed on social media.

## **6. Parent social media use**

Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school.

Parents will be asked not to share any photos or personal details of pupils when commenting on school social media sites, nor post comments concerning other pupils or staff members, in accordance with the Social Media Code of Conduct for Parents.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the Head of School, and may have their ability to interact with the social media websites removed.

Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution.

## **7. Pupil social media use**

Pupils will not access social media at any point during the school day.

Pupils will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Where a pupil or parent attempts to "friend" or 'follow' a staff member on their personal account, it will be reported to the Head of School.

Pupils will not post any content online via their personal social media account which is damaging to the school or any of its staff or pupils. Pupils will not post anonymously or under an alias to evade the guidance given in this policy.

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

Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to exclusion

## **8. Online safety**

Any disclosures made by pupils to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour will be reported to the Head of School, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Dealing with Allegations of Abuse Against Members of Staff and Volunteers Policy, and Disciplinary Policy and Procedures. If the concern is about the Head of School, it will be reported to the chair of governors.

Concerns regarding a pupil's online behaviour will be reported via the online safeguarding reporting tool to the DSL, who will investigate any concerns with relevant staff members, e.g. the Head of School and ICT Technician, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Head of School will contact the police. The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

As part of the usual communication with parents, the school will reinforce the importance of pupils being safe online and inform parents what systems the school uses to filter and monitor online use. The school will also make it clear to parents what their children are being asked to do online for school, including what sites they will be asked to access and who from the school, if anyone, they will be interacting with online.

## **9. Blocked content**

In accordance with the school's Online Safety Policy, the ICT Technician will install filtering systems on the school's network to prevent access to certain websites.

The ICT Technician retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

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

Inappropriate content accessed on the school's internet will be reported to the ICT Technician so that the site can be blocked.

## **10. Cyberbullying**

Cyberbullying incidents are taken seriously at Damers First School. Any reports of cyberbullying on social media platforms by pupils will be handled in accordance with the Anti-bullying Policy.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Allegations of cyberbullying from staff members will be handled in accordance with the Dealing with Allegations of Abuse Against Members of Staff and Volunteers Policy.

## **11. Training**

The school recognises that early intervention can protect pupils who may be at risk of cyberbullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils. Teachers and support staff will receive training on social media as part of their new starter induction. Teachers and support staff will receive annual and ongoing training as part of their development.

Pupils will be educated about online safety and appropriate social media use on a termly basis through a variety of mediums, including assemblies, PSHE lessons and cross-curricular links. Pupils will be provided with material to reinforce their knowledge.

Parents will be invited to online safety and social media training on an annual basis and provided with relevant resources, such as our Social Media Code of Conduct for Parents.

Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

## **12. Monitoring and review**

This policy will be reviewed every two years by the Head of School, in conjunction with the ICT Lead, ICT Technician and DPO.

The next scheduled review date for this policy is **November 2024**.

Any significant changes made to this policy will be communicated to all staff, pupils and parents.

# Photography/Video at Damers

The use of photography/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras, iPads and other recording devices to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons or for staff training purposes.

We also take images of your child using school devices as evidence of their work, which are inserted into their exercise books, as part of our everyday practice. Occasionally images will be of groups of children from across the class; your child may be in a group with others or in the background of another child's image.

Images may also be used to celebrate success through their publication in newsletters, on the school website, class blogs and occasionally in the public media.

The school will comply with the General Data Protection Regulation and ensure that when images are published that the children can not be identified by the use of their full names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Schools within Wessex Multi-Academy Trust will always ask for permission for visual images to be recorded. Also, we will not make any audio recording without informing you. In the same way, should it be necessary to make a recording, we also expect parents/carers to request permission for any recordings made on the school site or in the course of school business.

For further information please see our privacy notice available on our website.

**Please complete the form overleaf** to allow the school to take and use images of your child. If you have any questions about any of the above then please contact the school office.

**Name of child** .....

**Class** .....

**Name of parent/carer** .....

<b>Photography/Video For Use Outside School</b>					
I agree to Damers First School taking digital/video images of my child and agree to the following usage (please tick <b>Yes</b> or <b>No</b> ): <sup>1</sup>				<b>Yes</b>	<b>No</b>
School website					
Class blog					
Official class photo <sup>2</sup>					
Individual photo <sup>2</sup>					
School Newsletter					
Video hosting website <sup>3</sup>					
Dorset Echo publications <sup>4</sup>					
Poundbury / Celebrating Poundbury Magazine and website <sup>4</sup>					
DASP and DASP Music websites <sup>4</sup>					
Wessex MAT website <sup>4</sup>					
Learning Ladders <sup>5</sup>					
Signed				Dated	
Relationship to child					

<b>Taking Photographs/Video of My Own Child</b>			
I agree that if I take digital/video images at, or of, school events which include children other than my own, I will abide by these guidelines overleaf in my use of these images.			
Signed			
		Dated	
Relationship to child			

## Notes

<sup>1</sup> If you change your mind, please email [office@damers.dorset.sch.uk](mailto:office@damers.dorset.sch.uk), telephone 01305 264924 or visit the school office and we will update your consent form.

<sup>2</sup> Individual photos, your child's class photos and your child's performance DVD are taken by school photographers. Individual photos are uploaded to our school management system and photo printing services. Individual photos, your child's class photos and your child's performance DVD will be available for you to purchase.

<sup>3</sup> We use vimeo.com to upload and display selected videos.

<sup>4</sup> Where the Wessex MAT or press use their own photographer, consent will be requested by them for specific events.

<sup>5</sup> Learning Ladders is an online tool for teachers to track Foundation children's progress. Images of your child, either on their own or in a group, will be uploaded to Learning Ladders. You will be invited to a session with your child's teacher where you can learn more about Learning Ladders.