

Northchapel Community Primary School Digital and Social Media Policy

Review Date	Autumn 2023
Reviewed By	Deborah Coggin
Approved By	Andy Tate
Due for next review	Autumn 2024

Aim of this policy

- is to maintain the School’s duty to safeguard children (in line with the current version of Keeping Children Safe in Education), the reputation of the School and those who work there and the wider community of parents from the many issues that can arise as a result of use of photographs and posts on social networking sites and any other digital media.
- is to ensure safe use of digital and social media and minimise the risks to Northchapel Primary School.
- it deals with all of the forms of digital and social media including: Facebook, Twitter and Instagram and any other social networking sites in use by staff, governors, parents and pupils, as well as the school website and assessment apps such as Tapestry.
- the policy covers all employees, consultants, contractors, volunteers, casual workers, agency workers and governors, as well as children, their parents and the wider community.

Staff/Governors

- Staff/governors will not accept friend requests from current pupils, or ex-pupils under the age of 13.
- If staff/governors receive a friend request from a child, they will notify that child’s parents and school leaders.
- Staff/governors will correspond with school and parents through official school email addresses and not through any social media networks.
- Staff/governors will not discuss anything to do with school, pupils or other staff members, or post photos of school events on personal social media sites unless they are linking to or sharing the official school social media page. Staff/governors may find it helpful to have separate social media accounts which they use when interacting on school social media sites to avoid tricky situations of privacy.
- Staff/governors will ensure they have the tightest privacy settings possible on personal accounts but also understand that anything posted on social media has the potential of becoming public so must maintain a personal high standard of professionalism.
- Staff will not use personal social media on school devices, or on personal devices while responsible for children during working hours.
- Complaints against staff or allegations of misconduct regarding social media will be dealt with in accordance with the appropriate county policies.

Parents

- We request that parents do not post photos, videos or comments that include other children at the school on their personal social media accounts, including Whatsapp, as there may be restrictions parents are unaware of.
- Parents must not access social media while helping at school or on school visits (see Parent Helpers Guidelines).
- We ask parents to raise queries, concerns and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g. groups set up for school parents to communicate with each other) or on the school's pages.
- Any posts by parents or community that appear to be malicious regarding the school, its staff, governors or pupils will be dealt with in the following way:
 - Where there are allegations that a comment has been made that is malicious or detrimental to the school, the parent/s will be invited in to discuss their concerns directly and may be asked to remove the comment.
 - Comments that are threatening, abusive, racist, sexist or that could be seen as a hate crime will be reported to the police as online harassment.

Children

- The School will teach and review safety online each term and have regular reminders to children about how to keep themselves safe. Lessons will also include how to behave online, what to do if they are upset or concerned by comments online and how to report online bullying or harassment.
- Children should follow the age guidelines and restrictions for social networking sites (13 for most sites including Facebook and Instagram, 16 for Whatsapp).
- Tell their parents if they are using the sites, and when they are online.
- Be aware how to report abuse and inappropriate content.
- Not access social media on school devices unless directed by a member of staff.
- Not make inappropriate comments (including in private messages) about the school, teachers or other children.

School

- Northchapel School host a Facebook page, an X account and an Instagram page and the PTA host a Facebook page. The School also has a website hosted by e4education. These sites are open to the public and is for the purpose of promoting the School and sharing School activities and information. Designated staff and parents will have access to these sites and will manage and upload content.
- The School recognises for a number of safeguarding reasons sometimes it is necessary **not to** include children on social media. Parents will be asked to give permission for photos of their children to be used on these sites and are able to refuse consent. However, please be aware refusal of consent can cause distress for children if they have to be removed from group photos so we ask parents to carefully consider reasons if they wish to refuse consent and discuss this with the School. Consents given can be given/withdrawn at any time by writing to Mrs Vanessa Semmens, Data Protection Officer at the school address or alternatively, by email: office@northchapelprimary.co.uk.
- Photos will also be used in our prospectus and in local newspapers and Parish magazines. Parents are asked to give permission for this use of images of their children.

- The School will only post positive and promotional photos that show children sharing their learning or successes. The School will never use full names of children alongside their photos and generally no names will be used. On some occasions we may use first names to celebrate a child's success or achievement.
- Other photos of children will be taken for the purpose of displays in school and for learning observations as part of our assessment processes, as well as Health and Safety and Safeguarding duties.
- The School will always act in a manner to safeguard children and remain within the protocol of the guidelines in the most up to date version of Keeping Children Safe in Education (see Government website).
- Please be aware it is not possible for any organisation to fully control reproduction of published images.

Appendix – Policy to be followed in the case of a pandemic or school closure (remote learning)

Leadership Oversight and Approval

- Remote learning will take place using ClassDojo and Microsoft Teams.
 - ClassDojo and Microsoft Teams has been assessed and approved by the headteacher.
- Staff will only use Northchapel managed or specific, approved professional accounts with pupils and parents/carers. It is recommended staff use Northchapel managed systems where possible.
 - Use of any personal accounts to communicate with pupils and/or parents/carers is not permitted.
 - Any pre-existing relationships or situations which mean this cannot be complied with MUST be discussed with Deborah Coggin, Designated Safeguarding Lead (DSL).
 - Staff will use work provided equipment where possible e.g. a school/setting laptop, tablet or other mobile device. If this is not provided, leaders should ensure clear expectations are in place in relation to safeguarding and data security when using personal devices e.g. using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.
- Online contact with pupils and parents/carers will not take place outside of the operating times as defined by SLT:
 - 8:30am – 5:00pm
- All remote lessons will be clearly uploaded to the class page on ClassDojo; a member of SLT, DSL will have full access and is able to drop in at any time.
- Live streamed remote learning sessions will be held in agreement with the headteacher and adhere to our 'Live Sessions' guidelines for staff, parents and pupils.
- Live streamed meeting via Teams can be used for the staff and governors to communicate and hold meetings.

Data Protection and Security

- Any personal data used by staff and captured by ClassDojo when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
- All remote learning and any other online communication will take place in line with current Northchapel Primary's confidentiality expectations as outlined in our Data Protection policy.
- Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
- Only members of Northchapel School community will be given access to ClassDojo.
- Access to ClassDojo will be managed in line with current IT security expectations as outlined above in this policy.
 - Staff expectations e.g. using strong passwords, logging off or locking devices when not in use etc.

Session Management

- Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
 - language filters, disabling/limiting chat, staff not permitting pupils to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.
- A pre-agreed invitation/email (relevant to Microsoft Teams) detailing the session expectations will be sent to those invited to attend.
 - Access links should not be made public or shared by participants.
 - Pupils and parents/carers should not forward or share access links.
 - If pupils/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the class page.
- Alternative approaches and/or access will be provided to those who do not have access. School will provide devices where they feel appropriate and as constrained by limited stocks.

Behaviour Expectations

- Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
- All participants are expected to behave in line with existing Northchapel policies and expectations. This includes:
 - Appropriate language will be used by all attendees.
 - Staff will not take or record images for their own personal use.
 - Pupils and parent/carers cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.
- Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the remote learning.
- When sharing videos, participants are required to:
 - Wear appropriate dress.
 - Ensure backgrounds of videos are neutral (blurred if possible).
 - Ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
- Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

- Participants are encouraged to report concerns during remote learning:
 - Insert specifics or reference where to find them. For pupils, schools could insert age/ability appropriate details e.g. reporting concerns to the member of staff running the session, telling a parent/carer etc.
- If inappropriate online language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the Headteacher and parent/carers.
- Inappropriate online behaviour will be responded to in line with existing policies such as Digital and Social Media Policy, Whistleblowing policy, Relationships and Behaviour policy.
 - Sanctions for deliberate misuse may include: restricting/removing use, contacting police if a criminal offence has been committed.

Digital and Social Media Policy

- Any safeguarding concerns must be reported to Deborah Coggin, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Northchapel Digital and Social Media Acceptable Use Policy (AUP) for remote learning.

Staff Member Name:

Date.....