NORTH HAVEN SCHOOL

POLICY

May 2024

# SOCIAL MEDIA POLICY

## Scope

This policy applies to all staff, volunteers and contractors working in a school, preschool or corporate setting who use a social media platform in their professional capacity, or who identify themselves as a school, preschool or corporate employee, volunteer or contractor in a personal capacity. It assists staff who use social media to:

- engage internally with staff or with the wider community as a communications tool
- showcase children and students' work
- integrate with, and facilitate, teaching and learning
- administer social media platforms in an authorised capacity, or make contributions in a professional or personal capacity on education-related issues.

## Rationale

The intention of this policy is to establish a culture of transparency, trust and integrity in social media activities and to encourage the integration of social media into our teaching and learning environments.

This policy recognises that all communication by department staff will comply with the standards of conduct and behaviour as outlined in the Code of Ethics for the South Australian Public Sector.

The social media guideline is based on the Department for Education policy and outlines the practical implications of introducing and managing social media platforms. It also provides information for staff to help children and young people in the application and safe use of social media and should be considered alongside existing cyber safety resources.

## Detail

When setting up and maintaining social media, you must adhere to the ICT cyber security standard (PDF 485 KB) . The NHS ICT acceptable use policy reinforces the type of behaviours that are appropriate when using departmental ICT facilities and services. The North Haven School written agreement signed by staff, students, parents and guardians *(as appropriate)* must be adhered to. (NHS Staff ICT Acceptable Use Acknowledgement and Student ICT Acceptable Use Acknowledgement).

Schools should not endorse companies, products, opinions or causes unless an official endorsement already exists. For guidance on this issue, refer to the DPC Circular 023: Private Sector Endorsements on Government Public Communications (PDF 46KB).

If staff notice inappropriate or unlawful online content relating to the department or school, or content published in breach of this policy, report it to the Principal and Communications directorate at Education.SocialMedia@sa.gov.au.

## Principal:

The principal will ensure that IT requirements for establishing social media activities and profiles are in place.

North Haven School's Facebook and Instagram pages are managed and monitored by the principal. The principal has the ultimate responsibility of all content posted on the school's Facebook and Instagram pages and will manage breaches of policy in a timely manner.

Teachers do have access to this page upon request to the Principal or through the Facebook/Instagram delegate/manager, for the purpose of promoting student achievement or connecting with the wider school community around class events.

Department employees are responsible and accountable for official business transactions over social media and are to make sure records are kept and captured into an approved record keeping system located centrally at their site.

**The Principal**

- broadly consults with the community affected by social media before establishing new media use.
- ensures cyber-safety use agreements are in place for all staff and young people.
- ensures staff understand and comply with this policy.
- provides relevant training to carers, teachers and young people who will be using social media.
- ensures protective practices are in place to safeguard carers, teachers and young people.
- provides processes for staff and young people to identify and report offensive online material or behaviour.
- acts quickly to remedy issues when they arise and support staff and young people through these processes.
- models best practice in social media usage.
- ensures that IT access has appropriate safeguards in place to protect all young people.
- Provides students with regular cyber-safety messages via teachers teaching the curriculum and external professionals, i.e. SAPOL visits.

## Staff

All staff must maintain a professional relationship with students. Protective practices for staff and their interactions with children and young people (PDF 3 MB) guides staff to establish and maintain appropriate boundaries. Most importantly, teachers and SSO'S must not have children or young people in their education community as 'friends' on their personal or private social media sites.

When creating or posting to a social media platform that officially represents the department, school or preschool, staff must:

- ensure NHS Staff ICT Acceptable Use Acknowledgement is completed before a user is given access to systems. User agreements must be re-signed if any major changes are made to the agreement or if the staff member has been involved with any disciplinary action involving their unacceptable use.
- ensure approval has been granted for social media activity from the Principal.
- teach topics contained in keeping safe: child protection curriculum.
- teach strategies to maintain a positive online presence and protect identity.
- teach children and young people how to identify and avoid inappropriate materials.
- ensure the school conforms with government branding standards that clearly identifies the school.

- be aware of the specific social media channels and etiquette, and understand the views and feelings of the target community.
- ensure that they do not digitally published student photos without parent/guardian permission.
- staff to be provided with a class/school list of students who do not have parent permission for the publication of their identity.
- ensure all material published is respectful of all individuals, the department and the specific social media site and its community guidelines.
- moderate discussions and comments appropriately.
- not publish any material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, a breach of a court suppression order, or is otherwise unlawful or inappropriate.
- ensure that all content published is accurate and not misleading.
- ensure all information posted or comments made on government policy:
  - ➢ is appropriate to the individual's area of expertise and authority.
  - ➢ remains politically neutral.
  - ➢ does not breach the Code of Ethics for the South Australian Public Sector.
  - ➢ does not breach any confidentiality guidelines.
  - ➢ is not the first or a significant announcement on a topic (unless specific permission has been given).
- respect copyright and intellectual property requirements and attribute work to the original source wherever possible.
- protect personal details.
- gain consent to publish an individual's media or creative work as per the consent to use media and creative work procedure.
- use government branding in accordance with the Government of South Australia branding guidelines (PDF 2869KB) where required.
- ensure any young people involved understand the rules of operation of each social media site and measures are in place to protect them from any potential risks.
- must ensure processes appropriately address the needs of vulnerable children, including those children in state care.
- keep and dispose of records in accordance with the Information and Records Management Policy, ensuring appropriate records are created and captured for all business functions, activities and transactions. Where official records are created on electronic media including websites and social media, they should be treated no differently than an official record in any other format.
- Department employees are responsible and accountable for official business transactions over social media and to make sure records are kept and captured into an approved record keeping system located centrally at their site.

## Children and young people

- follow North Haven School's cyber-safety use agreement.

- ensure NHS Student ICT Acceptable Use Acknowledgement is completed before a user is given access to systems.  User agreements must be re-signed if any major changes are made to the agreement or if the student has been involved with any disciplinary action involving their unacceptable use.
- avoid any involvement with material or activities that could put personal safety at risk, or the privacy, safety or security of the school or other members of the school community.
- apply cyber-safety strategies and instructions when using social media.

## Related policies

Social media guideline
NHS Staff ICT Acceptable Use Policy
NHS Student ICT Acceptable Use Policy
ICT cyber security standard (PDF 485 KB)
Information and records management policy.
Code of Ethics for the South Australian Public Sector.
Keeping safe: child protection curriculum
The department ICT security policies, standards and procedures
Acceptable Use Policies for Schools, Preschools and Children’s Services Sites Standard
Information and records management policy

Reviewed:  May 2024    Governing Council approved:  14 / 05 / 2024