



Unlocking the full potential in everyone

Diverse - Research - Culture - Enhance - Community

Head Teacher
Omar Jennings

Assistant Head
Andrea Rantell

Nightingale Primary School

Acceptable Use Policy

This policy does not require a signature. Expectations apply automatically to all users.

Purpose of This Policy

This Acceptable Use Policy sets out the expectations for anyone using digital technology, devices, online platforms or internet access at Nightingale Primary School.

It applies to:

- Pupils
- Staff
- Governors
- Volunteers
- Visitors
- Contractors
- Parents/carers when using school platforms

By entering the school, using our devices, or accessing our systems, all users are considered to have understood and agreed to follow this policy.

1. Principles

We expect all users to:

- Use technology **safely, responsibly, and respectfully**.
- Protect personal information—your own and others’.
- Behave online in a way that upholds Nightingale’s values.
- Report anything that feels unsafe, inappropriate, or worrying.
- Understand that online activity may be monitored for safety.

2. Expectations for Pupils

Pupils must:

Safe Use

- Use school devices and platforms only for learning.



Unlocking the full potential in everyone
Diverse - Research - Culture - Enhance - Community

Head Teacher
Omar Jennings

Assistant Head
Andrea Rantell

- Keep passwords private and secure.
- Tell an adult if something online makes them uncomfortable.

Respectful Behaviour

- Be kind, polite and respectful in all digital communication.
- Never damage devices or change settings.
- Never take photos/videos of others without permission.

Responsible Online Conduct

Pupils must NOT:

- Access or search for inappropriate content.
- Use abusive, unkind or threatening language.
- Attempt to bypass filters or monitoring systems.
- Share personal information (name, address, passwords).
- Bully, harass or embarrass others online.
- Copy or use someone else's work without permission.

Online behaviour expectations apply **in and out of school** if behaviour affects pupils or staff at Nightingale.

3. Expectations for Staff

Staff must:

Professional Use

- Use school systems for school-related work.
- Use school communication tools—not personal accounts—to contact pupils.
- Keep passwords secure and never share login details.
- Follow safeguarding procedures for reporting concerns.

Role-Model with Technology

Staff must:

- Supervise pupils carefully when using devices.
- Model safe, ethical and respectful behaviour online.
- Use school-approved platforms and avoid unverified apps/tools.

Information Security

Staff must NOT:

- Store sensitive data on unencrypted devices.



Unlocking the full potential in everyone
Diverse - Research - Culture - Enhance - Community

Head Teacher
Omar Jennings

Assistant Head
Andrea Rantell

- Share confidential information through personal accounts.
- Install unauthorised software or apps.
- Disable monitoring, filtering or security tools.

4. Expectations for Parents/Carers

Parents and carers are expected to:

- Support safe digital behaviour at home.
- Use school platforms respectfully (ClassDojo, email, Google Classroom).
- Avoid posting images of other children online.
- Contact the school with any safeguarding concerns.
- Model appropriate behaviour when communicating online.

Parents must NOT:

- Use school platforms for complaints—these should follow school procedures.
- Share private or confidential information about staff or children.

5. Expectations for Visitors and Volunteers

Visitors and volunteers must:

- Use school devices only under staff supervision.
- Refrain from photographing pupils unless authorised.
- Follow staff guidance on safeguarding.
- Not access personal social media while working with children.

6. Use of Senso Monitoring Software

Nightingale uses **Senso** to support safeguarding.

All users must be aware that:

- School devices are monitored.
- Senso flags concerning or unsafe behaviour.
- Screenshots may be taken when risk is detected.
- Alerts are sent to the Designated Safeguarding Lead (DSL) team.

Monitoring operates **8am–5pm on school days**.

Misuse of school devices will be investigated.

7. Digital Safety and Security

All users must:

- Keep devices secure and report damage immediately.
- Respect filtering and monitoring settings.



Unlocking the full potential in everyone
Diverse - Research - Culture - Enhance - Community

Head Teacher
Omar Jennings

Assistant Head
Andrea Rantell

- Avoid clicking suspicious links or attachments.
- Use strong passwords and log out when finished.

8. Use of Personal Devices

Pupils

- Pupils may not use mobile phones during the school day.
- Phones must be switched off and stored safely if brought to school.

Staff

- Personal devices must never be used to communicate with pupils.
- Staff must follow the school's mobile phone policy.

Visitors

- May only use devices in accordance with school safeguarding rules.

9. Use of Images and Video

All users must follow these rules:

- Pupils must not take photos or videos of others without permission.
- Staff must only take images for educational purposes.
- Images must only be stored on school systems.
- Parents must not share images containing other children online.

10. Breaches and Consequences

Breaches of this policy may result in:

- Temporary or permanent loss of device access
- Behaviour or disciplinary procedures
- Parental meetings
- Removal from school platforms
- Referral to the Designated Safeguarding Lead
- In serious cases, police involvement

The school's decision is final.

11. Reporting Concerns

All users must report:

- Inappropriate behaviour



Unlocking the full potential in everyone
Diverse - Research - Culture - Enhance - Community

Head Teacher
Omar Jennings

Assistant Head
Andrea Rantell

-
- Unsafe content
 - Cyber-bullying
 - Suspicious online contact
 - Damage or technical issues

Reports should be made to the **Designated Safeguarding Lead (DSL)** or any trusted adult.

12. Review of Policy

This Acceptable Use Policy is reviewed **annually**, or sooner if required due to:

- New technologies
- Emerging online risks
- Updates to safeguarding guidance
- Behaviour trends

Issued: November 2025	Omar Jennings
Review Date: November 2026	