Janvrin School

Janvrin School Staff Responsible Use Agreement (RUP)

May 2027

Applies to: All employees, supply staff, volunteers, governors, students on placement, contractors and visitors with access to school systems.

---

1. Purpose

Janvrin School is committed to ensuring that digital technologies are used safely, responsibly and effectively to support teaching, learning, communication and administration.

This agreement sets out the standards expected of all staff when using:

- School networks and internet services
- Office 365 and associated cloud services
- Email and messaging systems
- School devices and personal devices used for work purposes
- Digital communications
- AI-enabled technologies
- Photographs, videos and other digital media
- Personal and sensitive data

All staff are required to read, understand and sign this agreement before being granted access to school ICT systems. [Janvrin Sc...2026 .pdf], [gov.je]

---

2. Professional Responsibilities

I understand that:

- My use of school technology must support my professional duties.
- I am responsible for safeguarding children while using digital technologies.
- I must comply with school policies, CYPES guidance, data protection requirements and safeguarding procedures.
- My use of school systems may be monitored and recorded for safeguarding, security and operational purposes. [Janvrin Sc...2026 .pdf], [gov.je]

---

3. Account Security

I agree that I will:

-

- Keep my username and password secure.
- Never share passwords with another person.
- Use strong passwords and multi-factor authentication where available.
- Lock my device whenever it is unattended.
- Report any suspected account compromise immediately.
- Not attempt to access systems or information for which I am not authorised. [Janvrin Sc...2026 .pdf]

---

4. Acceptable Use of School Systems

I will:

- Use school ICT primarily for educational and professional purposes.
- Access only material that is appropriate and relevant to my role.
- Respect copyright and intellectual property rights.
- Follow all software licensing requirements.
- Use cloud storage and collaboration tools only as authorised by the school.
- Ensure that digital resources used with pupils are appropriate for their age and learning needs. [Janvrin Sc...2026 .pdf]

I will not:

- Access, create, store or distribute inappropriate, offensive or illegal content.
- Install unauthorised software or applications.
- Attempt to bypass filtering, monitoring or security controls.
- Use school systems for personal commercial activity.
- Deliberately introduce malware or harmful code. [Janvrin Sc...2026 .pdf], [gov.je]

---

5. Safeguarding and Monitoring

I understand that:

- Monitoring systems may generate alerts relating to online activity.
- Any safeguarding concern identified through technology use must be reported immediately to the Designated Safeguarding Lead (DSL).
- Concerns involving online abuse, harmful content, inappropriate contact, cyberbullying, grooming or exploitation must be treated as safeguarding matters.
  Digital evidence must be preserved and not deleted if it may be required for investigation. [Janvrin Sc...2026 .pdf], [gov.je]

---

6. Communication with Pupils and Families

I will:

- Use only approved school communication systems.
- Maintain professional boundaries at all times.
- Ensure communication is appropriate, transparent and related to school business.
- Follow school expectations regarding email, Office 365, Google Workspace, InTouch and other authorised platforms. [Janvrin Sc...2026 .pdf]

I will not:

- Use personal email accounts to communicate with pupils.
- Use personal social media accounts to communicate with pupils.
- Share personal telephone numbers unless specifically authorised by school procedures.
- Engage in private online discussions with pupils outside approved systems. [Janvrin Sc...2026 .pdf]

---

7. Mobile Devices

Where personal devices are authorised for work purposes, I will:

- Protect devices with a PIN, password or biometric security.
- Keep devices updated.
- Store school information securely.
- Report loss or theft immediately.

I understand that school-related information must not be saved on personal devices unless authorised and adequately protected. [Janvrin Sc...2026 .pdf], [gov.je]

---

8. Data Protection and Confidentiality

I will:

- Handle personal information lawfully and securely.
- Access personal data only when required for my role.

- Use approved storage solutions.
- Take reasonable steps to prevent unauthorised disclosure.
- Report any suspected data breach immediately.

I will not:

- Share confidential information with unauthorised individuals.
- Transfer sensitive information using unsecured methods.
- Download or retain personal information unnecessarily. [Janvrin Sc...2026 .pdf], [gov.je]

---

9. Use of Artificial Intelligence (AI)

When using AI tools approved by the school, I will:

- Maintain confidentiality and data protection requirements.
- Not enter identifiable pupil data into unapproved AI systems.
- Verify the accuracy of AI-generated content before use.
- Apply professional judgement at all times.
- Ensure AI supports teaching and administration rather than replacing professional responsibility. [gov.je]

---

10. Images, Video and Media

I will:

- Use school-approved devices for photographs and recordings wherever possible.
- Follow parental consent arrangements.
- Store images securely.
- Ensure any publication of images follows school procedures.

I will not:

- Use images in a way that could put a child at risk.
- Share pupil images on personal social media.
- Publish identifying information alongside pupil photographs. [Janvrin Sc...2026 .pdf]

---

11. Social Media

I understand that:

Online conduct can affect public confidence in the school.
- Content posted online may remain publicly accessible.

I will:

- Maintain professional standards online.
- Avoid posting content that could bring the school into disrepute.
- Follow school and CYPES social media guidance.

I will not:

- Identify or discuss pupils, families or colleagues inappropriately online.
- Share confidential school matters through social media. [Janvrin Sc...2026 .pdf], [gov.je]

---

12. Reporting Concerns

I will immediately report:

- Safeguarding concerns
- Cyberbullying incidents
- Security breaches
- Suspected malware or phishing
- Inappropriate online material
- Data breaches
- Lost or stolen devices containing school information

Reports should be made to the DSL, Headteacher, Digital Safeguarding Lead or other designated person in accordance with school procedures. [Janvrin Sc...2026 .pdf], [gov.je]

---

13. Breaches of This Agreement

I understand that failure to comply with this agreement may result in:

- Removal of ICT access rights
- Internal investigation
- Disciplinary action
- Referral to external agencies where appropriate

This will be managed in accordance with school, CYPES and applicable legal procedures. [gov.je], [Janvrin Sc...2026 .pdf]