

Scratch

Submitting Controller

Name of controller	Nene Valley Partnership
Subject/Title of DPO	DPO
Name of controller contact / DPO	Warwickshire DPO Service
Date of last review	06/02/2026

The Nene Valley Partnership operates a cloud first approach to software procurement, which requires careful consideration of the privacy implications of such systems. This Data Protection Impact Assessment (DPIA) provides a structured process for identifying, assessing, and addressing or mitigating privacy risks, and helps us understand the long-term implications of any proposed or existing system.

Moving to cloud-based services has significant data protection implications. To manage these effectively, the trust must maintain a clear understanding of how information flows through its systems. This DPIA examines the broader privacy context, considering Data Protection Law, the Human Rights Act, and the practical need for cloud hosted solutions. It also evaluates the potential impact on individual privacy.

As part of this process, the trust must identify:

- Where data is stored
- How data can be transferred
- What control and access the school retains over its data

The trust will also ensure that the cloud provider's security measures are adequate and that the rights of data subjects under UK GDPR are upheld.

The Nene Valley Partnership intends to review and update this DPIA annually.

A DPIA will normally include the following key steps:

1. Identify the need for a DPIA
2. Describe the information flow
3. Consultation process (unless system already in place)
4. Assessing necessity and proportionality
5. Identify data protection and related risks
6. Identify solutions to reduce or eliminate those risks
7. Sign off the outcomes of the DPIA.

To assist with completing this document, please view the guide attached to the bottom of this this document template

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Scratch Online IDE will be used by students across the Nene Valley Partnership to support the computing curriculum. The system supports the creation of individual student accounts and involves the processing of usernames, passwords, and user-generated digital project content.

A DPIA is required because the processing involves:

- Children, who are a vulnerable data subject group
- A cloud-hosted system outside the direct control of the Nene Valley Partnership
- Potential data exposure through public-facing interactive features
- A platform that allows communication between users, which may create privacy risks if not adequately restricted

The DPIA ensures risks are identified and mitigated.

Step 2: Describe the processing

Describe the nature of the processing

How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Students will access Scratch using accounts created and configured by staff.

The processing includes:

- Collecting student usernames (non-identifiable naming convention)
- DOB field is present, but this is randomly generated with non-specific date
- Setting and managing passwords
- Storing student-created project content
- Sharing of projects on the Scratch platform
- Deletion of data when accounts are no longer required/reached end of enrolment

Accounts are created manually by a member of staff, usernames are anonymised.

Data, in the form of ‘projects’, are added to the website and created by the student. No intentional high-risk processing (e.g., special category data) occurs. All data is stored on Scratch’s cloud infrastructure.

Deletion

The data retention period for this platform - is held for the period of time that a student is on roll at the establishment, this would be 7 years at a primary school and 8 years at a secondary school.

Describe the scope of the processing

What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Data types: student username, password, project content

- No special category data is required or collected
- Creation of accounts: a one-time assignment/account creation per student, is actioned when it is required when Scratch homework begins.
- Volume: the use of this software is at the discretion of the teacher and the data could scale to 2000+ students (Year N–14) and 300+ workforce members across the Trust (NVP).
- Data submission: students use/create ‘projects’ within Scratch during lessons and homework activities
- Retention: accounts retained for the duration of use and deleted when a student leaves the institution.
- Geographical scope: usage across Nene Valley Partnership schools; storage location determined by ‘[Scratch’s hosting arrangements](#)’ – see section “International Cross-Border Data Transfer” for elaborated information.

Describe the context of the processing

What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The processing occurs within the established relationship between the Nene Valley Partnership and its students.

Key contextual considerations:

- Children are a vulnerable data group
- Students may share personal information inadvertently
- Scratch includes community features (commenting, public sharing) that create exposure to external users
- The platform is widely used in education but requires careful consideration to ensure safety

Control of Personal Data

Scratch is used to support the student's learning and is part of the computing curriculum, we do not ask students for their personal identifiable information, account names are randomised and contains no identifiable labels, therefore, students have limited control of their account and can only delete 'projects' that are associated with their own provided account.

A parent can request their student assigned Scratch account, is deleted once their student leaves the institution, of which, this occurs at the end of their active enrolment.

Expected Use of Data

Scratch is platform chosen to be used within the computing curriculum. Creating 'projects' on this platform is a formalised process for delivering and learning the computing curriculum.

Any known risks and mitigations – Use table below – add cells as needed

Issue	Risk	Mitigation
Student comments	Students may include personal data (name, address) in comments on projects	Disable commenting where possible; issue guidance to students on appropriate use; monitor use in class and at home
External user interaction	Scratch users outside of the organisation may comment on student profiles or projects	Lock down accounts; restrict sharing; teacher supervision in classroom
Project content	Students may embed identifying information within their own projects	Provide guidance; ensure staff review and monitor project submissions

Describe the purposes of the processing

What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing - for you, and more broadly?

The purpose is to support curriculum delivery by enabling students to:

- Develop programming skills
- Demonstrate creativity and problem-solving
- Save and manage coding projects in a digital environment

The processing benefits the Nene Valley Partnership by delivering statutory computing education and providing modern learning tools.

The intended effect on individuals is improved digital literacy, coding competence, and responsible online engagement.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Consultation Externally:

Consultation to students and parents is not required as this service falls under "Article 6(1)(e)" as this is necessary for the school to perform its official functions, i.e. delivery of the curriculum.

Consultation Internally:

Consultation between the ICT curriculum and senior leaders at the institution to determine suitability and use of the software within the curriculum.

Consultation with External Processors:

Documentation on the Scratch website was used to inform the decision of the appropriateness in using Scratch as part of the computing curriculum.

Consultation with Security Experts:

There is no plan to consult within information security experts.

If the system or its processing activities change in the future, the trust will conduct further consultation with relevant stakeholders to ensure transparency and maintain compliance with data protection obligations.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Lawful basis: Public Task (Article 6(1)(e)) - processing is necessary for providing statutory education.

The processing is necessary to deliver the computing curriculum

Proportionality measures include:

- Use of non-identifiable usernames
- Minimal data collection (only login credentials and project content)
- Restrictions on community features
- The platform's privacy notice explains their data usage/processing
- Systems to support individuals' rights, including account deletion and correction
- No international transfers beyond vendor hosting arrangements; data is stored according to Scratch's standard compliance processes
- Monitoring of compliance through ongoing reviews

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Students posting personal data in comments	Possible	Low	Low
External users commenting on student projects	Possible	Low	Low

Students embedding identifying data in project content	Possible	Low	Low
--	----------	-----	-----

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Students posting personal data	Disable comments; provide guidance; monitor activity	Reduced	Low	Yes
External user contact	Restrict sharing; use privacy configurations; disable public interaction; monitoring during class use	Reduced	Low	Yes
Identifying data in projects	Staff guidance; review of projects before sharing	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	09/02/26	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Please see comments added to the document and template prompts where further information is required.		
DPL Reviewed:	27 th February 2026	D. Thacker
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA