



Data Protection Policy

Approved by: Board of Directors

Policy Owner: Storyy Education

Responsible Senior Lead: Natalie Lee

Date Approved: August 2026

Review Cycle: Annually and as required

Next Review Date: August 2027

Version: 2.0

Contents

Contents.....	2
1. Why this policy exists	3
2. Who this policy applies to	3
3. Data Protection Principles.....	4
4. Lawful Basis for Processing	5
5. Confidentiality	5
6. Information We Keep	6
7. Sharing Information with Third Parties	7
8. Responsibilities.....	7
8.1 The Directors are responsible for:	7
8.2 The Data Protection Lead is responsible for:.....	8
8.3 Managers are responsible for:	8
8.4 All Staff are responsible for:	8
9. General Staff Guidelines.....	8
10. Data Storage	9
10.1 Paper Records	9
10.2 Electronic Records.....	9
11. Data Use and Handling.....	9
Remote Working and Mobile Devices	10
Artificial Intelligence (AI).....	10
Cyber Security	11
Reporting a Data Breach	11
12. Subject Access Requests (SARs)	12
13. Individual Rights.....	12
14. Redactions and Exemptions.....	13
15. Complaints	13
16. Monitoring and Compliance	13
17. Policy Review	14

1. Why this policy exists

Storyy Education collects and processes personal information in order to provide high-quality education and support services, safeguard children and young people, meet our legal and contractual obligations, and effectively manage the organisation.

This policy ensures that Storyy Education:

- Complies with all relevant data protection legislation and follows recognised best practice.
- Protects the privacy and rights of children, young people, parents/carers, staff, volunteers and partner organisations.
- Is transparent about how personal information is collected, used, shared, stored and disposed of.
- Maintains appropriate security measures to protect personal information from unauthorised access, loss, misuse or disclosure.
- Supports lawful and proportionate information sharing where necessary to safeguard children or meet statutory responsibilities.
- Reduces the risk of personal data breaches.
- Provides individuals with information about their rights under data protection legislation.
- Demonstrates accountability by maintaining appropriate records, policies and procedures relating to data protection.

The person responsible for data protection within Storyy Education will oversee compliance with this policy, monitor changes in legislation and guidance, support staff, respond to Subject Access Requests and coordinate the management of any personal data breaches.

2. Who this policy applies to

This policy applies to:

- Storyy Education Head Office.
- All Storyy Education provisions.
- Directors.
- Senior Leaders.
- Provision Managers.
- Employees.
- Volunteers.
- Agency workers.
- Contractors.
- Consultants.
- Students on placement.
- External professionals working on behalf of Storyy Education.

- Third-party organisations processing information on behalf of Storyy Education.

This policy applies to all personal information processed by Storyy Education, regardless of whether that information is stored electronically, on paper, by photograph, CCTV, video, audio recording or any other format.

Personal information may include, but is not limited to:

- Names.
- Dates of birth.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- Emergency contact details.
- Photographs.
- CCTV footage.
- Medical information.
- Educational records.
- Attendance information.
- Behaviour records.
- Safeguarding information.
- Employment information.
- Payroll information.
- DBS and safer recruitment documentation.
- Financial information.
- Online identifiers.
- Any information capable of identifying an individual.

3. Data Protection Principles

Storyy Education will ensure that all personal information is processed in accordance with the principles set out within UK GDPR.

Personal information will be:

- Processed lawfully, fairly and transparently.
- Collected only for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.

- Accurate and kept up to date.
- Kept only for as long as necessary.
- Stored securely using appropriate technical and organisational safeguards.
- Protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

Storyy Education is committed to demonstrating accountability for compliance with these principles through appropriate governance, training, policies, monitoring and record keeping.

4. Lawful Basis for Processing

Storyy Education will only process personal information where there is a lawful basis for doing so.

Depending on the purpose of processing, this may include:

- Compliance with a legal obligation.
- Performance of a contract.
- Legitimate interests pursued by Storyy Education or another organisation.
- Protection of an individual's vital interests.
- Performance of a task carried out in the public interest.
- Consent, where consent is the most appropriate lawful basis.

Where Storyy Education processes special category data (such as health, safeguarding or ethnicity information) or criminal offence information, an additional lawful condition under the Data Protection Act 2018 will also be identified.

Consent will only be relied upon where appropriate and individuals will always be informed of their right to withdraw consent where consent is the lawful basis.

5. Confidentiality

Within Storyy Education we respect confidentiality in the following ways:

- Personal information will only be shared with individuals who have a legitimate professional reason to receive it.
- Information relating to a child or young person will ordinarily only be shared with their parent or carer where appropriate and lawful.
- Information provided by parents, carers or professionals will not be shared with third parties unless there is a lawful basis for doing so.
- Information may be shared without consent where necessary to safeguard a child or young person, prevent serious harm, comply with a legal obligation or support a criminal investigation.

- Safeguarding and child protection records will be stored securely and shared only with the Designated Safeguarding Lead (DSL), Deputy DSLs and other authorised professionals on a strict need-to-know basis in accordance with Storyy Education's Safeguarding and Child Protection Policy.
- Data protection legislation will never be used as a reason to withhold information where sharing that information is necessary to safeguard or promote the welfare of a child.
- Staff will only discuss personal information where it is necessary to support education, safeguarding, planning, wellbeing, health and safety or operational requirements.
- Staff will be made aware of their responsibilities regarding confidentiality during induction and through ongoing training and supervision.
- Employment matters relating to staff, volunteers and contractors will remain confidential to those with responsibility for managing employment matters.
- Personal information will be stored securely using approved systems including SharePoint, Storyy Education's CRM, CPOMS and other authorised systems with appropriate access controls.
- Staff must not discuss confidential information in public areas or where conversations may be overheard.
- Confidential documents must be stored securely when not in use and disposed of in accordance with Data Retention guidelines.

6. Information We Keep

Storyy Education will only collect and retain personal information that is necessary to provide education and support services, safeguard students, manage employment relationships and meet our legal, contractual and regulatory responsibilities.

This information may relate to:

- **Children and young people** – including personal details, educational records, attendance, behaviour, safeguarding information, medical information, risk assessments, incidents and accidents.
- **Parents and carers** – including contact details, emergency contacts, consent forms and communication records.
- **Staff, volunteers and contractors** – including recruitment records, employment information, payroll, training records, DBS information and occupational health information where appropriate.
- **Schools, Local Authorities and partner agencies** – including referral information, commissioning arrangements, contracts and professional contact details.

Storyy Education will ensure that all personal information is accurate, relevant and kept up to date. Information will only be retained for as long as necessary in accordance with legal requirements and Storyy Education's Records Retention Schedule. When records are no longer required, they will be securely destroyed or permanently deleted.

7. Sharing Information with Third Parties

Storyy Education recognises that appropriate information sharing is essential to safeguarding students, supporting education and fulfilling our legal responsibilities.

Personal information will only be shared where there is a lawful basis to do so and where the information shared is necessary, relevant, accurate and proportionate.

Information may be shared with:

- Parents and carers.
- Commissioning schools.
- Local Authorities.
- Children's Social Care.
- Health professionals.
- The Police.
- The Local Authority Designated Officer (LADO).
- HMRC and pension providers.
- Approved payroll, IT and software providers.
- Other statutory or regulatory agencies where required.

Information relating to safeguarding concerns may be shared without consent where this is necessary to protect a child or another individual from harm, comply with a legal obligation or support a criminal investigation.

Where information is shared without consent, the decision and reasons for sharing will be recorded where appropriate.

Storyy Education will ensure that any third-party organisation processing personal information on our behalf has appropriate contractual agreements and security measures in place to comply with data protection legislation.

8. Responsibilities

Everyone working for or on behalf of Storyy Education has a responsibility to protect personal information and ensure it is handled securely and appropriately.

All staff will receive data protection training during induction and regular refresher training thereafter.

8.1 The Directors are responsible for:

- Ensuring Storyy Education complies with data protection legislation.
- Approving policies and procedures.
- Providing appropriate resources to support compliance.

- Monitoring organisational risks relating to data protection.

8.2 The Data Protection Lead is responsible for:

- Monitoring compliance with data protection legislation.
- Providing advice and guidance to staff.
- Coordinating Subject Access Requests.
- Managing and investigating personal data breaches.
- Reviewing policies and procedures.
- Liaising with the Information Commissioner's Office (ICO) where required.
- Supporting staff through training and ongoing advice.

8.3 Managers are responsible for:

- Ensuring staff understand and comply with this policy.
- Monitoring the secure handling of personal information.
- Reporting any concerns or suspected data breaches immediately.
- Supporting staff with information governance queries.

8.4 All Staff are responsible for:

- Protecting confidential information.
- Only accessing information required for their role.
- Keeping passwords and devices secure.
- Following approved procedures for storing and sharing information.
- Reporting suspected data breaches immediately.
- Completing mandatory data protection training.
- Seeking advice if unsure how to handle personal information.

Personal information must never be accessed, shared or used for personal reasons or outside an individual's authorised role.

9. General Staff Guidelines

All staff have a responsibility to ensure that personal information is handled securely, accurately and confidentially at all times.

When working with personal information, staff must:

- Only access information required to carry out their role.
- Keep all personal information confidential and only share it with authorised individuals on a need-to-know basis.
- Ensure information is accurate and updated where necessary.
- Immediately report any concerns regarding the security or misuse of personal information.

- Follow Storyy Education's policies and procedures for storing, sharing and disposing of personal information.
- Complete mandatory Data Protection training and any refresher training required.
- Seek advice from their line manager or the Data Protection Lead if they are unsure how to manage personal information appropriately.

Personal information must never be accessed, shared or used for personal reasons or outside an individual's authorised responsibilities.

10. Data Storage

Storyy Education will ensure that all personal information is stored securely and protected against unauthorised access, loss, damage or misuse.

10.1 Paper Records

Where personal information is stored in paper format:

- Records will be kept in locked cabinets or secure rooms when not in use.
- Documents must not be left unattended in public areas, meeting rooms or on printers.
- Personal information must only be removed from the provision where authorised and necessary.
- Paper records that are no longer required will be disposed of using approved confidential waste or secure shredding.

10.2 Electronic Records

Electronic records will be stored securely using approved systems and appropriate security measures.

This includes:

- Password-protected computers and devices.
- Secure cloud-based systems, including Storyy Education's approved CRM, SharePoint and CPOMS.
- Role-based access controls to ensure staff only access information relevant to their role.
- Encryption where appropriate.
- Approved anti-virus software, firewalls and security updates.

Personal information must not be stored on personal devices, personal email accounts or unauthorised cloud storage platforms.

11. Data Use and Handling

When handling personal information, staff must ensure that information is only used for legitimate organisational purposes.

Staff must:

- Verify the identity of anyone requesting personal information before sharing it.
- Check recipient details carefully before sending emails containing personal information.
- Password protect or encrypt documents containing sensitive information where appropriate.
- Share only the minimum amount of information necessary.
- Ensure confidential conversations cannot be overheard by unauthorised individuals.
- Lock computer screens when leaving workstations unattended.
- Keep desks clear of confidential paperwork when unattended.
- Securely dispose of confidential information when no longer required.
- Avoid creating unnecessary duplicate records.

Storyy Education will take reasonable steps to ensure that all personal information remains accurate, relevant and up to date.

Remote Working and Mobile Devices

Where staff are authorised to work remotely, the same standards of confidentiality and data security apply.

Staff working away from a Storyy Education provision must:

- Only use Storyy Education-approved devices and systems where possible.
- Ensure devices are password protected and securely stored.
- Avoid accessing confidential information in public places where it may be viewed by others.
- Never leave devices or confidential paperwork unattended.
- Report any loss, theft or damage to devices immediately.

Personal information must not be downloaded or stored on personal devices unless specifically authorised.

Artificial Intelligence (AI)

Storyy Education recognises that Artificial Intelligence (AI) tools are becoming increasingly available to support administrative and educational tasks.

Staff must not enter confidential, identifiable or sensitive personal information relating to students, parents/carers, staff or partner agencies into any AI platform unless it has been formally approved by Storyy Education and appropriate data protection and security assessments have been completed.

Any use of AI must comply with this policy, Storyy Education's IT Acceptable Use Policy and all applicable data protection legislation.

Cyber Security

Storyy Education is committed to protecting personal information from cyber threats and unauthorised access.

Staff must:

- Use strong passwords that are unique to their Storyy Education accounts.
- Never share passwords with others.
- Use multi-factor authentication where available.
- Be alert to phishing emails and suspicious links.
- Report suspected cyber incidents immediately.
- Ensure software updates are completed promptly.
- Only install authorised software onto Storyy Education devices.

Regular cyber security measures, monitoring and updates will be implemented to help protect Storyy Education's systems and personal information.

Reporting a Data Breach

Storyy Education takes all personal data breaches seriously and is committed to responding promptly and effectively to minimise any potential risk to individuals.

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

Examples of a personal data breach include:

- Sending personal information to the wrong person.
- Losing paperwork or devices containing personal information.
- Unauthorised access to confidential information.
- Accidental deletion or alteration of records.
- Disclosure of confidential information to unauthorised individuals.
- Cyber security incidents, including phishing attacks or malware.

All staff must immediately report any actual or suspected personal data breach to the Data Protection Lead.

Data Breach Management

When a breach is reported, Storyy Education will:

- Take immediate action to contain the breach where possible.
- Assess the nature and potential impact of the breach.

- Record the breach in the Data Breach Log.
- Investigate the cause of the breach.
- Take appropriate action to reduce the risk of further breaches.
- Notify the Information Commissioner's Office (ICO) within 72 hours where required by law.
- Notify affected individuals where there is a high risk to their rights and freedoms.

Following any breach, Storyy Education will review its procedures, provide additional training where appropriate and implement any necessary improvements to prevent similar incidents occurring in the future.

12. Subject Access Requests (SARs)

Under UK GDPR, individuals have the right to request access to the personal information that Storyy Education holds about them.

Subject Access Requests may be made verbally or in writing and should be forwarded immediately to the Data Protection Lead.

Storyy Education will:

- Confirm the identity of the requester where necessary.
- Respond without undue delay and within one calendar month, unless an extension is permitted under data protection legislation.
- Provide information in a secure and accessible format.
- Explain where information cannot be disclosed due to a lawful exemption.

Parents/carers may request information relating to themselves and, where appropriate, information relating to their student.

Where a request relates to a student, Storyy Education will consider the student's age, understanding, best interests and any safeguarding concerns before deciding whether information should be disclosed.

Requests should be sent to:

Email: hello@storyy.group

13. Individual Rights

Storyy Education is committed to ensuring individuals can exercise their rights under UK GDPR.

These rights include:

- The right to be informed about how personal information is used.
- The right to access personal information.
- The right to request correction of inaccurate information.

- The right to request erasure of personal information where appropriate.
- The right to request restriction of processing.
- The right to object to certain processing activities.
- The right to data portability where applicable.
- The right to withdraw consent where consent is the lawful basis for processing.
- Rights relating to automated decision-making where applicable.

Some rights may be limited where Storyy Education has a legal obligation or lawful basis to continue processing personal information.

14. Redactions and Exemptions

Where Storyy Education receives a request for personal information, information will normally be disclosed unless a lawful exemption applies.

Examples of situations where information may be withheld or redacted include:

- Information relating to another identifiable individual.
- Information that may place a student or another individual at risk of harm.
- Information subject to legal professional privilege.
- Information that may prejudice the prevention or detection of crime.
- Information that is confidential under another legal exemption.

Each request will be considered individually, and Storyy Education will ensure any decision to withhold information is lawful, proportionate and appropriately documented.

15. Complaints

Anyone who is concerned about how Storyy Education has collected, used, stored or shared their personal information should contact the Data Protection Lead in the first instance.

All concerns will be investigated promptly and fairly in accordance with Storyy Education's Complaints Procedure.

If an individual remains dissatisfied with the outcome, they have the right to make a complaint to the Information Commissioner's Office (ICO).

16. Monitoring and Compliance

Storyy Education will regularly monitor compliance with this policy through:

- Regular policy reviews.
- Staff training and awareness.

- Data protection audits.
- Reviews of information security arrangements.
- Monitoring of data breaches and lessons learned.
- Reviews of data retention and disposal practices.

Any identified areas for improvement will be addressed promptly to ensure continued compliance with data protection legislation and best practice.

17. Policy Review

This policy will be reviewed annually, or sooner if required, following:

- Changes to legislation or statutory guidance.
- Changes to Storyy Education's systems or working practices.
- Significant data breaches or security incidents.
- Recommendations from the Information Commissioner's Office or other regulatory bodies.
- Organisational learning and continuous improvement.

Storyy Education is committed to maintaining the highest standards of data protection and information security to safeguard the personal information entrusted to us.