Storyy Group Data Protection Policy - UK GDPR and DPA 2018 (Reviewed 2025)

Storyy Group refers to the following sectors: Storyy Homes, Storyy AP and Storyy Training.

At Storyy Group (Storyy AP Ltd, Storyy Homes Ltd and Storyy Training Ltd) we respect the privacy of the young person attending our provisions, along with privacy of their parents or carers, as well as the privacy of our staff and all agencies we work with. Our aim is to ensure that all those using and working at Storyy Group do so with confidence that their personal data is being kept secure. We are registered with the Information Commissioners Office (ICO).

Storyy Group needs to gather and use certain information about individuals, this can include children a young person, parents, Local authority, employees and other people the organisation has a relationship with or may need to contact. This also includes names, dates of birth for the young person along with medical details, this is essential to ensure safeguarding of the welfare of all young persons in our care.

This policy outlines how the information is collated stored and handled to ensure that best practice is in place to protect sensitive data whilst complying with new laws and guidelines.

Why this policy exists?

Our updated GDPR & DPA 2018 Policy ensures that Storyy Group:

- Complies with the data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Our lead person for data protection is Ryan White. The lead person ensures that Storyy Group meets the requirements of the GDPR & DPA, liaises with statutory bodies when necessary, and responds to any subject access requests.

Who this policy applies to?

- The head office of Storyy Group.
- All staff and volunteers of Storyy Group.
- All contractors, suppliers and others working on behalf of Storyy Group.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR & DPA 2018.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs
- Medical information

- DBS and personal information
- Any other data we may collect.

Confidentiality:

Within Storyy Group we respect confidentiality in the following ways:

- We will only ever share information with a parent/carer about their own child/young person.
- Information given by parents/carer to staff about their child/young person will not be passed on to third parties without permission unless there is a safeguarding issue.
- Concerns or evidence relating to a child/young person's safety, will be kept in a confidential file and will not be shared within the provision, except with the DSL and manager. Relevant information on CP or safeguarding concerns will be shared with key individuals as per the Storyy Group Safeguarding and Child Protection Policy if and when it is needed.
- Staff only discuss an individual child/young person for purposes of planning, safety and group management.
- Staff are made aware of the importance of confidentiality during their induction process and through ongoing training and meetings.
- Issues relating to the employment of staff, whether paid or voluntary, will remain confidential to those making personnel decisions.
- All child/young person's personal data is stored securely electronically on password protected computers and restricted access CRM. This information is stored on a restricted usage Sharepoint server. CPOMS is used to report and store any further information. This will only be shared with relevant bodies in case of school transfer or reporting/safeguarding/child/young person protection.

Information that we keep:

The items of personal data that we keep about individuals are listed further below in this policy.

Child/Young person and parents: We hold only the information necessary to provide an alternative provision for each child/young person. This includes child/young person registration information, medical information, parent contact information, attendance records, incident and accident records and so forth. If you decide that your child/young person will no longer attend our provision we retain only the data required by statutory legislation and industry best practice, and for the prescribed periods of time. Electronic data that is no longer required will be deleted upon your request that your child/young person will no longer attend our provision; paper records are disposed of securely or returned to parents.

Staff: We keep information about employees in order to meet HMRC requirements, and to comply with all other areas of employment legislation. We retain the information after a member of staff has left our employment for the recommended period, then it is deleted or destroyed as necessary.

Key examples include:

- **Child / Young Person records:** Retained until the individual reaches 25 years of age (7 years after school leaving age) in line with safeguarding best practice.
- **Accident / incident records:** Minimum of 3 years, or longer if related to safeguarding.
- **Staff employment records:** 6 years after employment ends.
- **Payroll and tax records:** 6 years to comply with HMRC requirements.
- **Safeguarding records:** Retained in accordance with Local Safeguarding Partnership guidance (typically until the individual reaches 25 years).

Sharing information with third parties:

We will only share child/young persons information with outside agencies on a need-to-know basis and with consent from parents/career except in cases relating to safeguarding young person, criminal activity, or if required by legally authorised bodies (e.g., Police, HMRC, etc). If we decide to share information without parental consent, we will record this in the child/young person's file, clearly stating our reasons.

We will only share relevant information that is accurate and up to date. Our primary commitment is to the safety and well-being of the young person in our care.
Some limited personal information is disclosed to authorised third parties we have engaged to process it, as part of the normal running of our business, for example in order to take online bookings, and to manage our payroll and accounts. Any such third parties comply with the strict data protection regulations of the GDPR & DPA. Below is a summary of these third parties and our relationship with them.

Responsibilities:

Everyone who works for or with Storyy Group has some responsibility for ensuring data is collected, stored and handled appropriately. All employees have received GDPR & DPA training and is part of our induction process.

Each staff member that handles personal data must ensure that it is handled and processed in line with this policy and GDPR & DPA 2018 principles.

Whilst all staff members have a care of duty to ensure data is kept secure, below is an overview of specific responsibility.

The Directors are ultimately responsible for ensuring that Storyy Group meets its legal obligations.

The Data Protection Officer is Ryan White and is responsible for:

- Keeping the directors updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data Storyy Group holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The Directors are responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

Storyy Group will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below. In particular, strong passwords must be used, and they should never be shared with others.

Personal data should not be disclosed to unauthorised people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Storyy Group collects and uses personal data as a point of contact, safeguard young person, parents and staff at our provisions, inform of changes, report concerns and record activities.

General Staff Guidelines:

Data storage:

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer. We do not disclose this data to any third parties unless outlined in section 5.

- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot
- see it. (These guidelines also apply to data that is usually stored electronically but may also be printed, typically for registers.)

- When not required, the paper or files are kept in a locked drawer or filing cabinet.
- Employees make sure paper, and printouts are not left where unauthorised people could see them, like on a printer.
- If registers and personal data printouts are shredded and disposed of securely when no longer required.
- Contacting a customer or using their data in any way other than for the agreed purposes in line with Storyy Group's registration process is not accepted.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data is protected by strong passwords that are changed regularly and never shared between employees.
- Data is only stored on password protected computers, and via our third-party processing organisations (Section 5) if shared electronically with the child/young person's school it is password protected and stored in a secure place.
- Data is never saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data are protected by approved security software and a firewall.

Data use and handling:

When working with personal data, employees must ensure:

- The screens of their computers are always locked when left unattended.
- Personal data is not shared informally.
- Data must be encrypted before being transferred electronically. The DPO can explain how to send data to authorised external contacts.
- Data should not be transferred outside the UK unless adequate safeguards are in place in line with UK GDPR requirements.
- Employees should not save copies of personal data to their own computers.
- The law requires Storyy Group to take reasonable steps to ensure data is kept accurate and up to date.
- The more important it is that the personal data is accurate, the greater the effort Storyy Group should put into ensuring its accuracy.
- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Office staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the DPO's responsibility to ensure marketing databases are checked against our central database every 6 months
- All our staff are DBS checked and undergo training to ensure suitable handling and usage of data is being upheld.

Reporting a Data Breach:

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:

- Sending personal data to the wrong person
- Loss or theft of devices containing personal data
- Unauthorised access to data
- Accidental deletion or alteration of records

All staff must immediately report any data breach or suspected data breach to the Data Protection Officer (DPO).

- Who to contact: Ryan White (Data Protection Officer)
- How to report: Verbally (immediately) followed by an email summary outlining what has happened.

Data Breach Management Process:

Initial Report and Containment:

The staff member who identifies the breach reports it to the DPO without delay.
The DPO will assess the breach and take immediate steps to contain it where possible (e.g. recalling emails, securing access).

Logging the Breach:

The DPO will record the breach in the Data Breach Log, detailing:

- Date and time of breach discovery
- Nature of the breach
- Categories and approximate number of data subjects affected
- Categories and approximate number of personal data records affected
- Initial containment actions taken

Assessment and Risk Evaluation:

The DPO will use the ICO's personal data breach self-assessment tool to assess whether the breach needs to be reported to the ICO.

Notification:

If the breach poses a risk to individuals' rights and freedoms, the DPO will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will also be informed without undue delay, explaining:

- The nature of the breach.
- Contact details of the DPO.

- Likely consequences.
- Measures taken or proposed to address and mitigate the breach.

Investigation and Review:

The DPO will carry out a full investigation to identify root causes and implement corrective actions to prevent future breaches.
Outcomes and lessons learned will be shared with the Directors and relevant teams as part of ongoing compliance improvement.

Subject access requests:

- Parents/carers can ask to see the information and records relating to their child/young person, and/or any information that we keep about themselves.
- Staff and volunteers can ask to see any information that we keep about them.
- We will make the requested information available as soon as practicable and will respond to the request within one month at the latest.
- If our information is found to be incorrect or out of date, we will update it promptly.
- If any individual about whom we hold data has a complaint about how we have kept their information secure, or how we have responded to a subject access request, they may complain to the Information Commissioner's Office (ICO).
- Any requests for information or statements of withdrawal should be emailed to hello@storyy.group .

Redactions and Exemptions:

We will provide full access to personal data unless a lawful exemption applies, including:

- **Serious harm exemption:** If disclosure would be likely to cause serious harm to the physical or mental health of the requester or another person.
- **Third-party data:** Redact or withhold personal data about other identifiable individuals unless consent is obtained or disclosure is reasonable.
- **Confidential sources or information:** Where disclosure would reveal information given in confidence by another individual (not a professional), consider withholding unless consent is given.
- **Crime prevention:** If disclosure would prejudice the prevention or detection of crime
- **Legal professional privilege.**

GDPR:

We comply with the requirements of the GDPR & DPA, regarding obtaining, storing and using personal data. Our legal basis for processing the personal information relating to you and your child/young person is under your consent and for legitimate interests to allow us to keep you informed and safeguard your child/young person.

GDPR – Storyy Group use your personal data.

The company is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained within this document.

This notice applies to current and former employees, workers, and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles:

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept securely and for only as long as necessary for the purposes we have told you about.
- We process personal data in a manner that ensures it is secure and protected against unlawful or unauthorised processing, loss destruction or damage.
- We are responsible for and able to demonstrate compliance with these principles.

Types of data collected:

We collect and process personal data, including but not limited to:

Children and Young People:

- Name
- Date of Birth
- Contact information
- Educational, care and medical information
- Safeguarding data
- Behaviour and attendance records

Parents/Guardian/Carers:

- Contact information.
- Consent forms.
- Safeguarding information.

Staff and Volunteers:

- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.

- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.

Schools, Local Authority and external partners:

- Contact Information
- Payment details
- Contracts and service agreements

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Genetic information and biometric data.
- Information about criminal convictions and offences.
- CCTV footage (where applicable) and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider.

We may sometimes collect additional information from third parties including former employers, credit reference agencies (where applicable) or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you we will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract, we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. If you fail to provide personal information / if you fail to provide certain information when requested, we may not be able to perform the contract we have entered with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose:

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows.

Reviewed by Ryan White - 05/05/25
Next review – May 2026