storyybrook

Data Protection (GDPR) Policy

Contents

1. Purpose

The purpose of Storyybrook's Data Protection (GDPR) Policy is to ensure that all personal data is handled lawfully, fairly and securely, in line with statutory requirements and the expectations set out in the Staff Handbook .

At Storyybrook, we recognise that handling personal information is a fundamental part of safeguarding, professional conduct and effective school operation. This is particularly important within a specialist SEMH setting, where sensitive information is often required to support pupils' safety, wellbeing and educational progress.

This policy aims to:

- ensure compliance with data protection legislation
- protect the privacy and rights of pupils, staff and families
- support safe and appropriate information sharing
- maintain confidentiality and professional standards
- ensure data handling supports safeguarding and effective practice

All staff are responsible for understanding and applying this policy in their day-to-day role.

This policy is informed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope of this policy

This policy applies to all individuals working at or on behalf of Storyybrook, including teaching staff, support staff, leaders, volunteers and contractors.

It applies to all personal data processed by the school, including:

- pupil information
- staff records
- safeguarding information
- assessment and progress data
- communication with families and external agencies

This policy ensures that all data is handled consistently, securely and in line with the school's safeguarding responsibilities and professional expectations.

3. Key principles

All data at Storyybrook will be managed in a way that reflects the school's commitment to safeguarding, confidentiality and professional integrity.

Data protection will be managed in line with the following principles:

- Lawfulness, fairness and transparency – data will be processed appropriately and with clear purpose

- Purpose limitation – data will only be used for specific, legitimate purposes
- Data minimisation – only necessary information will be collected and used
- Accuracy – data will be kept up to date and accurate
- Storage limitation – data will not be kept longer than necessary
- Security – data will be stored and accessed securely
- Accountability – staff are responsible for handling data appropriately

At Storyybrook, staff understand that effective data handling supports safeguarding, communication and consistency across the school.

4. Data protection responsibilities

All staff have a responsibility to ensure that personal data is handled safely, securely and appropriately.

Staff must:

- only access data required for their role
- ensure information is accurate and up to date
- store data securely
- follow school procedures for sharing information
- report any concerns or breaches immediately

All staff receive data protection training as part of induction and regular refresher training thereafter. Additional guidance is provided where roles involve handling sensitive safeguarding or SEMH-related information.

Leaders are responsible for:

- ensuring systems and processes are in place
- providing guidance and training
- monitoring compliance

Failure to follow data protection expectations may result in disciplinary action in line with the Disciplinary Policy .

Data Protection Lead (DPL)

The school has a designated Data Protection Lead (DPL) responsible for overseeing compliance with data protection legislation, including the UK General Data Protection Regulation and the Data Protection Act 2018. The Data Protection Lead is responsible for ensuring that effective systems, processes and procedures are in place to support lawful, secure and consistent handling of personal data across the school. This includes monitoring compliance, providing guidance and training to staff, and ensuring that data protection responsibilities are clearly understood and implemented in practice. At Storyybrook, the DPL is the Headteacher, Mrs Rachel Burbridge.

The Data Protection Lead will act as the main point of contact for data protection matters, including responding to data breaches, managing Subject Access Requests

and liaising with external bodies such as the Information Commissioner's Office where required. They will ensure that data protection considerations are embedded within all aspects of school practice, particularly where information relates to safeguarding, staff conduct or sensitive pupil needs within the SEMH context.

The Data Protection Lead will also support leaders in reviewing and developing policies, maintaining appropriate records, and ensuring that data protection is applied in a way that is proportionate, transparent and aligned with the school's safeguarding responsibilities. All staff remain individually responsible for handling data appropriately; however, the Data Protection Lead provides oversight, support and accountability to ensure consistent and compliant practice across the school.

Data Protection Officer (DPO)

Storyybrook has appointed Brian Murphy as the designated Data Protection Officer (DPO). In his role as a Storyy Group Director, the DPO provides independent oversight and expert advice to ensure that the school meets its obligations under the UK General Data Protection Regulation and the Data Protection Act 2018.

The DPO is responsible for:

- monitoring compliance with data protection legislation and school policies
- advising the school on its legal responsibilities and best practice
- supporting the management of data breaches and Subject Access Requests (SARs)
- providing guidance and training to staff where required
- acting as a point of contact with the Information Commissioner's Office

The DPO operates independently from the school's day-to-day decision-making processes to ensure objective oversight and accountability. While the Data Protection Lead manages the operational implementation of data protection within the school, the DPO provides strategic guidance and challenge to ensure that data protection standards are consistently met.

All staff must cooperate with the DPO and follow any guidance provided to ensure that personal data is handled lawfully, securely and in line with the school's safeguarding responsibilities.

5. Lawful processing of data

Storyybrook will ensure that all personal data is processed lawfully, fairly and transparently, in line with the UK General Data Protection Regulation and the Data Protection Act 2018.

Personal data will only be processed where there is a clear and lawful basis. In a school context, the most common lawful bases include:

- Legal obligation – where the school is required to process data to comply with statutory duties (e.g. safeguarding records, attendance reporting, SEND documentation)

- Public task – where processing is necessary for the performance of the school's official functions (e.g. delivering education, recording progress, behaviour monitoring)
- Vital interests – where processing is necessary to protect a person's life or safety (e.g. emergency medical situations)
- Consent – where individuals have given clear permission for specific uses of their data (e.g. photographs, certain communications)

In practice, most data processed by the school will fall under legal obligation or public task, particularly where it relates to safeguarding, education and statutory responsibilities. Consent will only be used where appropriate and will not be relied upon where there is a clear imbalance of power or where the school has a legal duty to process the data.

Storyybrook recognises that much of the information processed within a specialist SEMH setting constitutes special category data, including safeguarding information, medical information, SEND records and sensitive personal information relating to pupils and families. This information requires enhanced protection, restricted access and careful handling to ensure confidentiality, safeguarding and compliance with data protection legislation.

Staff must ensure that:

- personal data is only used for its intended and lawful purpose
- only the minimum necessary information is processed
- decisions about data use are proportionate, relevant and justifiable

Storyybrook provides clear privacy notices explaining how personal data is collected, used, stored and shared. Privacy notices are available for pupils, parents/carers, staff, volunteers and visitors and are reviewed regularly to ensure accuracy and transparency.

Where there is uncertainty about the lawful basis for processing, staff must seek advice from the Data Protection Lead before using or sharing information.

In all cases, data processing must support safeguarding, effective practice and the best interests of pupils, in line with the school's safeguarding responsibilities.

6. Data security and storage

The school implements appropriate filtering and monitoring systems, secure password protocols and cyber-security measures to protect personal data and reduce the risk of unauthorised access, online threats or data loss.

All personal data must be stored securely to prevent unauthorised access, loss or misuse.

This includes:

- secure storage of paper records

- password-protected digital systems
- restricted access to sensitive information
- appropriate use of school systems and devices

The school will ensure that any third-party organisations, contractors or digital systems used to process personal data do so in compliance with the UK General Data Protection Regulation, the Data Protection Act 2018 and relevant contractual requirements. This includes systems used for safeguarding, assessment, communication, record keeping and school management.

Appropriate due diligence will be undertaken to ensure that external providers handle personal data securely, lawfully and in accordance with the school's safeguarding responsibilities.

Staff must ensure that:

- information is not left unattended
- devices are secure
- data is only accessed in appropriate settings

CCTV and surveillance systems

Storyybrook may use CCTV systems to support safeguarding, site security, behaviour monitoring and the protection of pupils, staff and visitors. Any use of CCTV will comply with the UK General Data Protection Regulation, the Data Protection Act 2018 and relevant guidance issued by the Information Commissioner's Office.

CCTV recordings will:
· only be accessed by authorised individuals
· be stored securely
· only be retained for an appropriate period
· only be used for lawful and proportionate purposes

Appropriate signage will be displayed across the school site to ensure transparency regarding the use of CCTV.

Requests to access CCTV footage, including Subject Access Requests, will be managed in line with statutory requirements and safeguarding considerations.

7. Confidentiality and information sharing

Confidentiality is a key expectation for all staff and is outlined within the Staff Code of Conduct. Staff must only use approved school systems and communication methods when handling personal data and must not share sensitive information through personal email accounts, messaging applications or unauthorised platforms.

Staff must:

- treat all personal information as confidential
- only share information on a need-to-know basis
- ensure that information is shared appropriately and securely

Information sharing must always be:

- proportionate
- relevant
- necessary

Where remote working is required, staff must ensure that personal data is accessed, stored and shared securely and in line with school procedures.

8. Data breaches

Any actual or suspected data breach must be reported immediately to the Data Protection Lead or a senior leader.

A data breach may include:

- loss of personal data
- unauthorised access or disclosure
- failure to follow data protection procedures

The school will:

- investigate the breach
- take appropriate action
- report to relevant authorities where required

Regulatory Authority and Reporting

Storyybrook recognises the role of the Information Commissioner's Office (ICO) as the UK's independent authority responsible for upholding information rights and enforcing data protection legislation.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the school will report the breach to the ICO without undue delay and, where required, within 72 hours of becoming aware of the breach, in line with statutory requirements.

The school will also cooperate fully with the ICO in the event of any investigation, enquiry or requirement for further information, and will ensure that all data protection practices are implemented in accordance with guidance issued by the regulator.

The school will also:

- assess the severity and impact of the breach
- take immediate steps to contain and mitigate any risk

- notify affected individuals where there is a high risk to their rights and freedoms
- maintain a record of all breaches, including actions taken and outcomes

All staff must report any actual or suspected data breach immediately to the Data Protection Lead to ensure that appropriate action can be taken promptly.

9. Safeguarding considerations

At Storyybrook, safeguarding is paramount and underpins all decisions relating to data and information sharing, in line with the Safeguarding and Child Protection Policy .

Staff must understand that:

- information sharing can be essential to protect a child
- data protection legislation does not prevent safeguarding action
- concerns must always be reported in line with safeguarding procedures

Where there is a conflict between confidentiality and safeguarding, the welfare of the child is the priority.

10. Individual rights

Individuals have rights in relation to their personal data, including:

- the right to access their data
- the right to request correction of inaccurate data
- the right to request deletion (where appropriate)
- the right to restrict processing

Requests will be managed in line with statutory requirements and within appropriate timescales.

Subject Access Requests (SARs)

Individuals have the right to request access to the personal data held about them. This is known as a Subject Access Request (SAR).

Requests may be made in writing or verbally and should be directed to the school's Data Protection Lead. The school will respond to all valid requests without undue delay and within one calendar month, in line with the UK General Data Protection Regulation.

Where necessary, the school may:

- request proof of identity to ensure that information is released securely
- seek clarification to ensure the request can be responded to appropriately
- extend the response period where requests are complex or multiple, in line with statutory guidance

Information will be provided securely and in a format that is accessible to the individual, unless an exemption applies.

In responding to requests, the school will ensure that:

- the rights of other individuals are protected
- safeguarding considerations are prioritised
- any disclosure is lawful, proportionate and appropriate

Staff must refer all Subject Access Requests to the Data Protection Lead immediately and must not respond directly unless authorised to do so.

11. Monitoring and review

Data protection practices will be monitored to ensure compliance and effectiveness.

This may include:

- review of data handling procedures
- monitoring of systems and access
- responding to incidents or concerns

Leaders will ensure that data protection is implemented consistently across the school.

12. Record keeping

Accurate and secure record keeping is essential to ensure compliance with data protection requirements and to support safeguarding and effective school operation.

Records will:

- be stored securely
- be retained in line with statutory guidance
- be accessible only to authorised individuals

All data will be managed in accordance with confidentiality and data protection requirements.

Storyybrook will ensure that personal data is not kept for longer than necessary and is retained in line with the UK General Data Protection Regulation, the Data Protection Act 2018, and relevant statutory guidance.

The school maintains a clear retention approach, ensuring that different categories of data are held only for appropriate periods. This includes, but is not limited to:

- Safeguarding records – retained in line with statutory safeguarding requirements and transferred securely when a pupil moves school
- Pupil educational records – retained for a defined period after the pupil leaves the school, in accordance with statutory guidance

- Staff personnel records – retained for a set period following the end of employment
- Attendance and assessment data – retained in line with operational and statutory requirements
- Medical information – retained for as long as necessary to support the safety and wellbeing of the individual

The school will:

- maintain a data retention schedule outlining specific retention periods for all categories of data
- regularly review stored data to ensure it remains necessary and appropriate
- securely dispose of data when it is no longer required, including shredding physical records and permanently deleting digital files

The school's detailed Data Retention Schedule is maintained separately and reviewed regularly to ensure ongoing compliance with statutory guidance.

All data retention and disposal decisions will be:

- lawful and proportionate
- consistent across the school
- aligned with safeguarding responsibilities

Staff must not retain personal data unnecessarily and must follow school procedures for the secure disposal of information.

13. Links to other policies

This policy should be read alongside:

- Staff Handbook
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Disciplinary Policy
- Low-Level Concerns Policy
- E-Safety Policy
- CCTV Policy

14. Summary statement

At Storyybrook, personal data is handled with care, professionalism and integrity. All staff are responsible for ensuring that information is managed securely, shared appropriately and used to support safeguarding, wellbeing and effective practice. Through consistent and responsible data handling, the school maintains a safe, respectful and compliant environment for all.

All staff must understand that failure to comply with data protection requirements may result in regulatory action as well as internal disciplinary procedures.