

Record Restriction Policy for LiquidLogic (Children's)

1. Policy Statement

Gloucestershire County Council provides services for people and local communities. The day-to-day work of the Council involves collecting and using information about the people whom we provide services to and with whom we work. Information from which an individual can be personally identified is protected by the Data Protection Act 2018. Under the Act, we have a legal duty to protect any information that we collect. We take measures to safeguard data and apply security standards and controls to prevent any unauthorised access.

Within Children's Services, there are occasions when we need to further limit access to the record of a child or family member. In these instances, Gloucestershire Children's Services will ensure that such records are 'Restricted' and only accessed by those members of staff directly involved with the care of that child/family.

There are two approaches to restriction of a record; **restricting access for an individual** where a record is only restricted to a named individual and **restricting access to a record** where all access is restricted. It should always be considered which approach is the most suitable for the circumstances and ensure the relevant criteria of the policy are met.

2. Purpose

The purpose of this policy is to provide a clear process for the restriction of access to records on LiquidLogic (LL) systems for Children's Services. This will include having a clear authorisation process with accountability from the manager along with a process for periodic review of these restrictions.

3. Record Restriction Criteria:

This policy should be followed when one of the following criteria is met:

Restricting access to a record

- Where disclosure of the adopter details could cause the breakdown of an adoption placement.
- Where there is a high-profile case - Public interest, where there may be a media interest.
- Where a serious case review is to be carried out.
- Where there is a sudden and unexplained death of a child, the LL support team have permission to lock the case immediately pending confirmation of the appropriate owner.
- Where the Head of Service (or member of Children's Services SLT) decides that information must be protected because of the sensitive nature of the case.

Restricting access for an individual

- Where a staff member is connected to a child or young person receiving a service or have knowledge that they received a service

4. Legal Context

The restriction of a record is put in place to protect the confidentiality of an individual. It does not impact on the access rights of the individual to request their information. This policy should be viewed within the context of the legislation and guidance for Information Governance and Children's Social Care as outlined below.

The Children Act 1989 and The Children Act 2004 - Sets out the responsibility of Councils with social care responsibilities to ensure that all children are safeguarded. This will require, in circumstances where children are thought to need additional services or at risk of significant harm, to undergo a formal assessment and where appropriate to arrange for the provision of social care services to meet the assessed needs of these children and their families.

Working Together to Safeguard Children 2018 - sets out how organisations and individuals should work together to safeguard and promote the welfare of children and young people in accordance with the legislation detailed above.

Data Protection Act 2018 / GDPR - This acts as a framework for the appropriate processing of data relating to individuals, including the obtaining, holding, use or disclosure of such information. Personal data must be processed in line with these requirements. This includes when data is shared or restricted.

Social Work England Codes of Practice – National codes of practice for social care workers and employers providing a clear guide for all those who work in social care, setting out the standards of practice and conduct workers and their employers should meet.

5. Process for enacting the policy

5.1 Request to Restrict Access

The criteria outlined above sets out the circumstances when a request to restrict access can be made. In such circumstances, and where workers or managers decide that the criteria are met to restrict a file the following procedure must be adhered to in all circumstances.

- Officers must discuss the circumstances for the child and reason for restricting the records with their line manager.
- Reminder: Priority consideration is to be given to restricting access for specific staff members rather than the whole record being restricted.

- Team Managers must request permission from their Head of Service to restrict the record; this should be done through a conversation.
- Team Manager to then completed Record Restriction Form on LL and Head of Service to approve. This form will then go to the ICT Application Support Team for action
- This form will be stored on the child's record as it notes the reason a restriction was put in place.

5.2 Exemptions to Restriction Process

Unless specifically refused, the following teams / job roles will be granted access to the restricted record:

- ICT Application Support Team
- System Owner
- Named Directors or Children's SLT members
- Emergency Duty Team (Permanent workforce)
- MASH – for named staff in the Triage

5.3 Accessing Restricted Records

When access is required for individual staff to access a restricted record this can be granted by emailing the ICT Application Support Team. Access to the restricted record and the authority to remove the restriction will sit with the current operational Head of Service for the child's record.

For restrictions of the full record there will be a 'lock' shown against the child and permission has to be sought to gain access. There are a limited number of occasions, where the information displayed in the lock notification could imply a child / young person's physical location in the County or the referral reason based on the name / team within the notification message. If this is the case, the notification details will be removed, and notes on who to contact held within the restricted area of the system. These instructions will instead direct to the ICT Application Support Team who will then coordinate accordingly. Examples include cases locked to the LADO (Local Authority Designated Officer) under the Allegation Management Procedure or adopted adults seeking birth records information. By doing this it avoids the risk of information being accidentally or partially revealed.

5.4 Reviewing Restricted Records

Restrictions of records should be reviewed at any point of change – when the team changes, the worker changes or the involvement is ended. The team manager should be asking the question at this stage about if the restriction is still required.

In addition, the restrictions should be reviewed every 6 months outside of any changes as above occurring.

If the decision is to remove the restriction then the Team Manager is to email the Head of Service who will complete the Record Restriction Form on LiquidLogic, requesting the option to remove the

restriction. ICT Application Support will then complete this action on the system and the form will be kept on the child's file to show the decision.

With respect to Serious Case Reviews, it will be necessary to keep the record 'restricted' until the outcome of the review is known and any criminal charges have been completed.

5.5 Restricted Records Reporting

A web report will be used to show record which have a full restriction applied. The restriction owner / Heads of Service are responsible for monitoring these restrictions and ensuring they are reviewed within timescales.

6. Monitoring and Review

This policy will be reviewed every 2 years and will be owned by the system owner and reviewed through the LL Prioritisation Group.

Policy Owner: Julie Miles (System Owner)

Policy Agreed: May 2021

Review Date: May 2023