Safeguarding Case Management System

Access Protocol

between

Flagg Nursery School (the School)

and

Derbyshire County Council (the Council)

1 Introduction

Schools are in a uniquely strong position to understand the safeguarding needs of children in their care and to proactively ensure that children in need of help and protection are provided with appropriate and responsive services. School staff play a particularly vital role in protecting children at risk of significant harm on child protection plans and in promoting improved education outcomes for children in care. This is recognised in the statutory responsibilities schools have with regard to safeguarding as set out in Section 175 of the Education Act 2002 (Section 157 gives the equivalent requirements for Academies and independent schools), which require them to "make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school".

In fulfilling these responsibilities schools are dependent on agencies sharing relevant information about children in a timely way. Serious Case Reviews have frequently pointed to the absence of appropriate information sharing with schools as a significant missed opportunity in protecting the child. The serious case review on the death of Daniel Pelka pointed to the absence of a shared understanding and knowledge of the child's behaviour in school and the involvement of Police and social care services with the family at home.

Providing Schools with access to the Council's Safeguarding Case Management System ("the System") provides an essential component in delivering improved safeguarding arrangements for children. The information contained within the system is by its nature highly sensitive and access to the System comes with a number of responsibilities and expectations. Access will only be provided following successful completion of relevant training by the designated users.

This protocol sets out how the School is permitted to use the System.

2 Commitments

The School commits to:

- Actively use the System as a method of addressing their overall safeguarding responsibilities, recognising that not using the System could be considered a failure of the safeguarding duty
- Ensuring that School staff granted access to the System are aware that their access will be recorded, monitored and/or reviewed.
- Ensuring that staff accessing the System always add a Case Note that details the reason for access.
- Having an ICT Acceptable Use Policy in place which has been provided to all staff. There should be a record within School to acknowledge receipt and awareness of the policy.
- Addressing inappropriate use of the System promptly and consistently through the School's disciplinary procedures
- Informing the Council immediately if there is detection, suspicion or the witness of an incident that may be a breach of the Data Protection Act 1998 or Computer Misuse Act 1990.

- Informing the Council when authorised users of the System leave the School
- Cooperating with the Council and the Information Commissioner's Office (ICO) in the event of a data breach
- Ensuring that only those employees authorised to use the System have signed and returned their personal commitment statements. Access will not be permitted for those who have not signed the agreement
- Ensuring that any Council equipment provided for the purpose of obtaining access to the System is subject to appropriate security precautions (e.g. kept in a safe and secure environment within the School premises, not left unattended or on display in a car such that it would encourage opportunist theft)
- Ensuring that the method by which the System connects to the Council's network is not interfered with or subverted.

3 Details of Key Commitments

3.1 Monitoring and Recording

Access to the System will be continuously recorded and stored in the System's audit logs. The audit logs will capture the date and time of individual transactions against the associated user ID and the parts of the System accessed. The Council will perform regular audits of access, which will include:

- Checking the records accessed by the School and confirming that each record access has a corresponding Case Note detailing the reason for access
- Identifying any irregular or inappropriate access
- Internal audit undertaking sample checks of the procedures in place at the School to manage the system access

Any actions that the Council considered inappropriate will be referred to the School and investigated further. This may result in a data breach being reported to the ICO and subsequent actions being taken.

3.2 Disciplinary Procedures

The Council expects that in the event of inappropriate use of the system, the school will follow its disciplinary procedures, taking into account the impact or potential impact that misuse of the data has caused.

Examples of inappropriate use of the system are:

- Viewing records of children or adults who have no relationship with the school (i.e. out of curiosity)
- Viewing records of children or adults without an associated justifiable safeguarding concern
- Not adding a Case Note detailing the reason for access for each record viewed
- Allowing someone else to use their access credential to log onto the System
- Accessing the system in a non-private location
- Using the system for personal gain/benefit or to further personal interests

- Not maintaining confidentially of information and personal data

3.3 Informing the Council of a Potential Information Breach

In the event of a potential data breach or inappropriate use of the system, the School must inform the Council immediately by ringing the Council's Service Desk on 01629 537777, ensuring the incident is noted as a potential security breach.

The incident will then be passed to the appropriate team and investigated.

3.4 Informing the Council that an Authorised User is Leaving the School

In the event of an authorised user leaving the employment of the School, the School must inform the Council by ringing the Council's Service Desk on 01629 537777, and providing the full name and user ID of the leaver.

If the Council has provided the leaver with any equipment to enable access to the System e.g. a token used as part of the system log on procedures, this must be returned to the Council by registered post to The Service Desk, Transformation Services, Derbyshire County Council, County Hall, Matlock, DE4 3AG.

3.5 Cooperation with the Council and the ICO

In the event of a reported security breach, the Council will investigate and determine if further action is required. The School is required to cooperate fully with the investigation, by providing the necessary information and assistance to complete the investigation in a timely manner.

Where the issue is reported to the ICO, the School is required to work closely with the Council to respond to the ICO in a timely manner.

Where the ICO finds that a data breach has occurred and a fine is imposed on the Council, the Council will seek to recover the full amount of the fine from the School where the School's employees or their actions have been deemed to be at fault for the breach

4 Agreement

The protocol should be signed by an appropriate signatory as specified in the School's delegated powers of authority. For example, if the signatory is defined as the Chair of Governors, the protocol should be signed by the Chair of Governors, acting on behalf of the School and formally recorded at the next Governing Body meeting, to ensure that all Governors are aware that the School has adopted the protocol.

We agree to adhere to the responsibilities and commitments detailed in this protocol.

Signed On Behalf of Flagg Nursery School
Signed_____ Title Chair of Governors Date_____ FGB Minute (if appropriate)