FRAMWELLGATE SCHOOL DURHAM

Title and Description	Data Protection Policy

Date of last review	June 2017
Approved by	Academy Trust Board
To be reviewed by	Academy Trust Board
Responsibility	Academy Business Director
Review period	Two yearly
Date of next review	June 2019

FRAMWELLGATE SCHOOL DURHAM

Data Protection Policy

1. Introduction

1.1. This Policy is related to the school's stated vision and values as well as its policy on 'Child Protection, Safeguarding and promoting the welfare of students' and 'Whistle Blowing'. Confidential information is information that is not normally in the public domain or readily available. It is information that has a degree of sensitivity and value. In the course of their work staff at FSD will, of necessity, be party to such information about students, their friends and family. This policy outlines the requirement of good practice for safeguarding confidentiality and sharing information.

1.2. It is a statutory requirement for all schools to have a Data Protection Policy: (http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

1.3. The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:

1.3.1. Personal data shall be processed fairly and lawfully;
1.3.2. Personal data shall be obtained only for one or more specified and lawful purpose(s);
1.3.3. Personal data shall be adequate, relevant and not excessive;
1.3.4. Personal data shall be accurate and where necessary, kept up to date;
1.3.5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
1.3.6. Personal data shall be processed in accordance with the rights of data
1.3.6.1. subjects under the Data Protection Act 1998;
1.3.7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
1.3.8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

2. Aims

2.1. The aim of this policy is to provide a framework to enable staff, parents and students to understand:

2.1.1. The law regarding personal data
2.1.2. How personal data should be processed, stored, archived and deleted/destroyed
2.1.3. How staff, parents and students can access personal data

3. Data Types

3.1. **Personal data**

3.2. The school has access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:-

3.2.1. Personal information about members of the school community – including students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records.
3.2.2. Curricular / academic data e.g. class lists, student progress records, reports, references
3.2.3. Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references

3.2.4. Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

3.3. **Sensitive Personal data**

3.4. Sensitive personal data is defined by the Act as information that relates to the following categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life, criminal offences/criminal proceedings. It requires a greater degree of protection and in a school may include:-

3.4.1. Staff Trade Union details
3.4.2. Information on the racial or ethnic origin of a child or member of staff
3.4.3. Information about the sexuality of a child, his or her family or a member of staff
3.4.4. Medical information about a child or member of staff
3.4.5. Information relating to any criminal offence of a child, family member or member of staff.

3.5. On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission may be sought from the parents / carers before posting information more widely, for instance in the staff room.

4. Privacy Statements

4.1. In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all students and staff of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be available via the school website, staff handbook and/or in paper copy on request.

5. Information and Sharing

5.1. The principles outlined below will help FSD staff to make informed decisions as to why they do or do not share information. This is needed in order to promote consistency and to deliver an effective service and appropriate support to our students and their families. Professional judgement will be needed unless there is a statutory duty or a Court Order to share.

5.2. Practice at FSD must be consistent with any relevant legislation and the statutory obligations of the Data Protection Act (1998), Human Rights Act (1988), and the Freedom of Information Act (2000). Reference will be made to the relevant legislation when appropriate.

5.3. Staff at FSD must not promise unconditional confidentiality. Any disclosure about behaviour which places the students, or others, at risk of significant harm may constitute a need to breach confidence. In such instances, reference should be made to the 'Child Protection, Safeguarding and promoting the welfare of students' policy.

5.4. All staff must pay due regard to only passing on information (verbally or in writing) to another person on a 'need to know' basis, and in compliance with this policy and privacy statements. In particular staff should not discuss students with the parents/carers of other students. If uncertain, advice is to be sought through the Academy Business Director in the first instance.

5.5. Staff should always consider how much information needs to be shared to achieve the objective and ensure that it is shared only with those people who need to have it.

5.6. Staff should always base their information sharing decisions on considerations of the safety and well-being of the student and others who may be affected by their actions.

5.7. Information recorded and shared should be accurate and up-to-date, be shared in a timely fashion and shared securely. In general, disclosures to external bodies / individuals should not be made over the telephone following an incoming call. Staff should phone back to a landline to verify the

identity of the caller or enquirers should be asked to submit their requests in writing (where appropriate on headed paper and/or by email) to allow checking of whether the request is legitimate. Wherever possible, replies should be in writing.

5.8. If in any doubt staff should seek advice from the Academy Business Director, or the County Council's Freedom of Information and Data Protection Co-ordinator at Durham County Council.

5.9. If the decision is to share, records should be made. (What was shared, with whom and for what purpose.) Likewise, a decision not to share should be recorded with the reason(s) for not sharing.

5.10. Parents/Carers may seek access to information held about their children who attend the school. A written request needs to be made to the Headteacher in such circumstances. Any access to information will only be granted if names (and other information) that would allow an individual other than their child(ren) to be identified is anonymised. (For example, witness statements from students should be typed with their names replaced 'Student A', 'Teacher A' etc.).

5.11. The school makes information public through its website as well as documents such as the Prospectus. Many documents, including School Policies are available on the website but can also be requested from the school. If the information isn't available on the website the school can be contacted to ask if it is available.

5.12. Details of how this policy is to be implemented is contained in the documents entitled, 'Protocol for Information Collection/Recording', 'Data Protection Flowchart' and the 'Taking Statements Flowchart'.

Data Security

5.13. All staff at FSD must pay due regard to the security of all records containing personal data, and sensitive data. Staff must take due care if personal data about staff or students is taken off the campus on laptops and/or data storages devices, and explicit permission to do this must be sought from the Head teacher.

5.14. When personal data is stored on any portable computer system, USB stick or any other removable media:

5.15. the data must be encrypted and password protected

5.16. the device must be password protected

5.17. the data must be securely deleted from the device once it has been transferred or its use is complete.

5.18. Staff must ensure the security of personal data (relating to students and staff) if taken off the school premises. Only staff who need to access records will be able to do so, with explicit permission from the Head teacher.

5.19. Images of students will not be processed off site, and will be protected and stored in a secure area.

5.20. All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts only.

5.21. E-mail cannot be regarded on its own as a secure means of transferring personal data. Where technically possible all e-mail containing sensitive information will be encrypted

5.22. The academy has clear procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. The academy will follow due diligence when selecting cloud based services, and ensure compliance with the requirements of the Data Protection Act as detailed in their guidance documents and via the following link.

5.23. http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

5.24. The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

5.25. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

5.26. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

6. Data Breaches

6.1. On occasion, personal data may be lost, stolen or compromised. A data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

6.2. Ransomware in itself may not be deemed as a data breach and a risk analysis should be undertaken in such circumstances before assessing whether a breach has occurred. This will involve the following assessment:

6.2.1. identify the number of affected data subjects

6.2.2. identify the records that have been accessed/subjected to the ransomware attack to establish what personally identifiable information may have been compromised (e.g. names, addresses, contact details);

6.2.3. identify if any sensitive personal data is included

6.3. There is currently no legal obligation on data controllers and data processors to report breaches of security which result in loss, release or corruption of personal data. The ICO believes serious breaches should be brought to its attention, however, by data controllers.

6.4. There is no definition of a serious breach but in its guidance Notification of data security breaches to the Information Commissioner's Office (ICO), the ICO identifies the following as considerations in assessing whether or not there has been a serious breach that should be reported, the:

6.4.1. potential detriment to data subjects;

6.4.2. volume of personal data lost/released/corrupted; and

6.4.3. sensitivity of the data lost/released/corrupted.

6.5. In the event of a potential data breach the Data Protection Officer will inform the head teacher and Chair of the Trust.

6.6. If deemed a breach, the academy will follow the relevant procedures in such instances as determined by the ICO.

7. Data storage, retention and deletion

7.1. Retention of Data

7.1.1. The guidance given by the Information and Records Management Society, and the Academy retention document will be referred to when retaining and destroying data.

7.1.2. Personal data that is no longer required will be destroyed and this process will be recorded. This should be treated as confidential waste.

7.1.3. Secure shredding will be done through use of shredding devices in school and/or through our contract with Riverdale Papers. For advice on this facility staff should contact the main school office in C Block.

7.1.4. Data should be stored securely in lockable storage if in paper format, and electronically in the correct locations on the network only accessible by appropriate staff.

7.1.5. For clarification on any data retention and deletion, advice should be sought from the Academy Business Director.

7.1.6. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

7.1.7. Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

7.1.8. Images must not be taken using personal cameras or phones.

7.1.9. The academy has clear procedures for the automatic backing up, accessing and restoring of all data held on school systems.

8. Third Party data transfers

8.1. As a Data Controller, the academy is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party ensuring their compliance with the Act.

9. Monitoring & Evaluation

9.1. This policy will be reviewed bi-annually as part of the policy review cycle by the appropriate member of the Senior Leadership Team and will be ratified by the appropriate Board or Committee as delegated.

9.2. This policy will be updated in the interim period should there be specific and significant changes to legislation during that period.

Draft: Revised – June 2017

Framwellgate School Durham

Protocol for Information Collection / Recording from Students

At Framwellgate School Durham, information collection and recording is essential for intervention purposes and preventative work for safeguarding and promoting the welfare of the students within our school.

There is an increasing emphasis on multi-agency working across integrated services in which our school plays a pivotal role. Therefore, any information collection or recording which informs this work must include relevant and accurate content and detail.

When collecting or recording information from students within school, the following guidelines are to be applied. Where the information applies to a Child Protection / Safeguarding Children issue, refer to the following guidelines.

The correct paperwork is used to collect / record information.

When there are incidents in lessons information is recorded on the school database and any student statements are recorded on a blank piece of A4 lined paper. Ensure it contains the detail outlined in point 2a.

When there are incidents around the campus, information is recorded using a Duty Slip and on the school database.

When statements are taken from students, this information is collected using a Recording Sheet.

All incidents are to be entered on the school database.

2a. The following information must be included in all written statements;

Full Name of Student
Tutor Group
Year Group
Date
Signature of all individuals collecting and recording information.

If a student names other student(s) ensure that full names are used.

2b. If these statements are then passed to an internal or external stakeholder for action the following information must be included;

A brief statement of how and when the evidence has been gathered
Name of person collecting / recording information and full names of all those involved.
Nature of incident / Reason for Referral / Other Circumstances
Signature of all individuals collecting / recording information and date

The information collected / recorded must be accurate and include facts not your personal opinion.

The language used in the collected / recorded information must reflect the intended audience. Ensure all language used is formal, full names and explanations provided. Be aware this information may be shared with a variety of internal and external stakeholders.

The information collected / recorded must be timely. It is important that all information is up-to-date and collected/recorded and if feasible on the same working day. A delay in completing relevant paperwork may compromise any outcome which could be achieved.

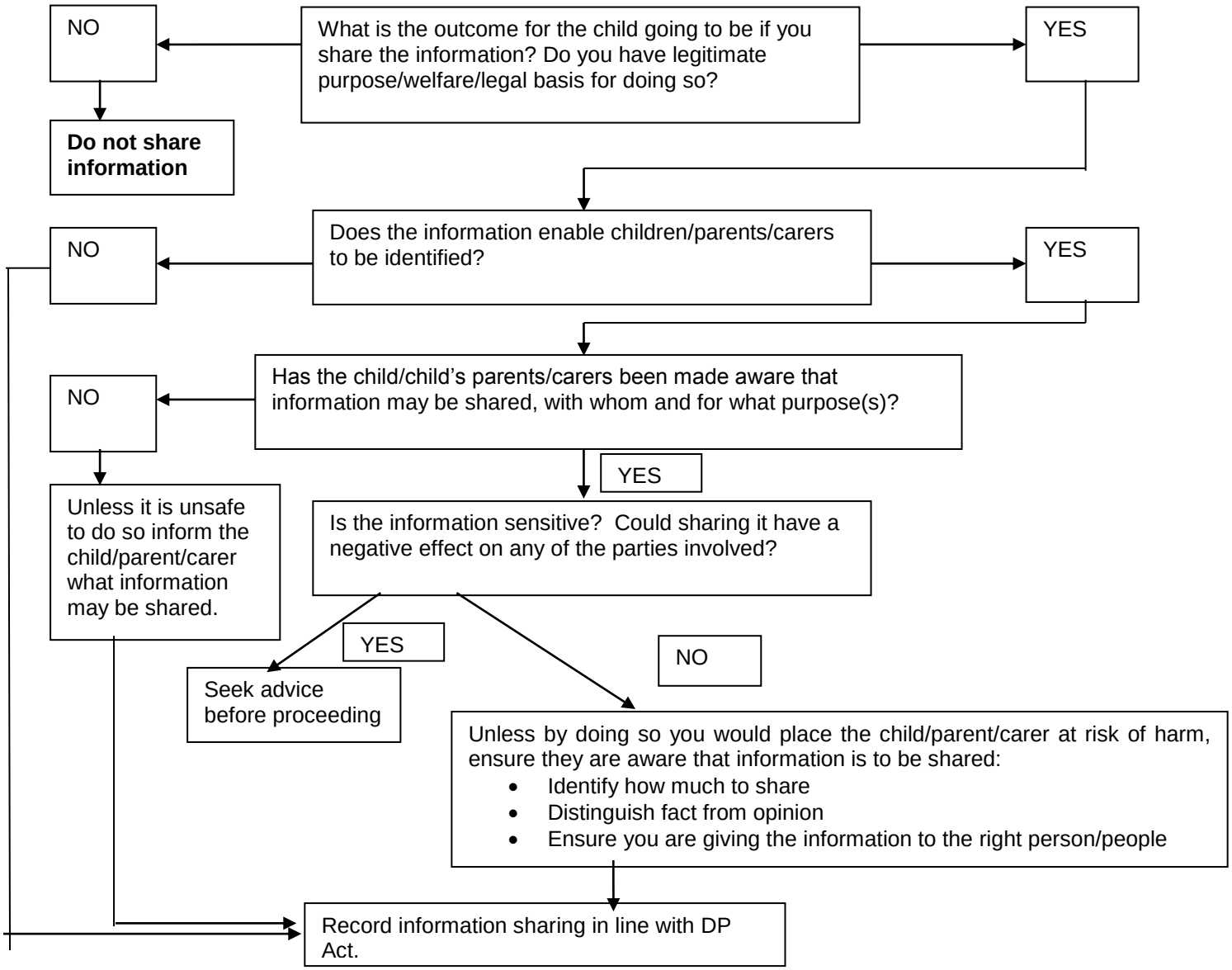
The individual receiving the collected information must record the action that is to be or has been taken and by whom and any relevant outcomes.

Data Protection Flowchart

Instances when you may wish to consult the Data Protection Flowchart:-

When speaking to colleagues about a student and/or parents/carers;
When taking a statement from a student following an incident;
In the case of a safeguarding or child protection issue;
If a student discloses information relating to his/her welfare either in school or outside of school;
When writing an incident report / reporting an incident in school/inputting incidents into the School Database;
When requested for information from people (e.g., parents and carers, external agencies) outside of school (often parents will ask for information about other students in the school).

If in doubt please consult the Designated Safeguarding Officer, the Student Services Manager or take advice from County Council's Freedom of Information and Data Protection Co-ordinator at County Hall before sharing information.

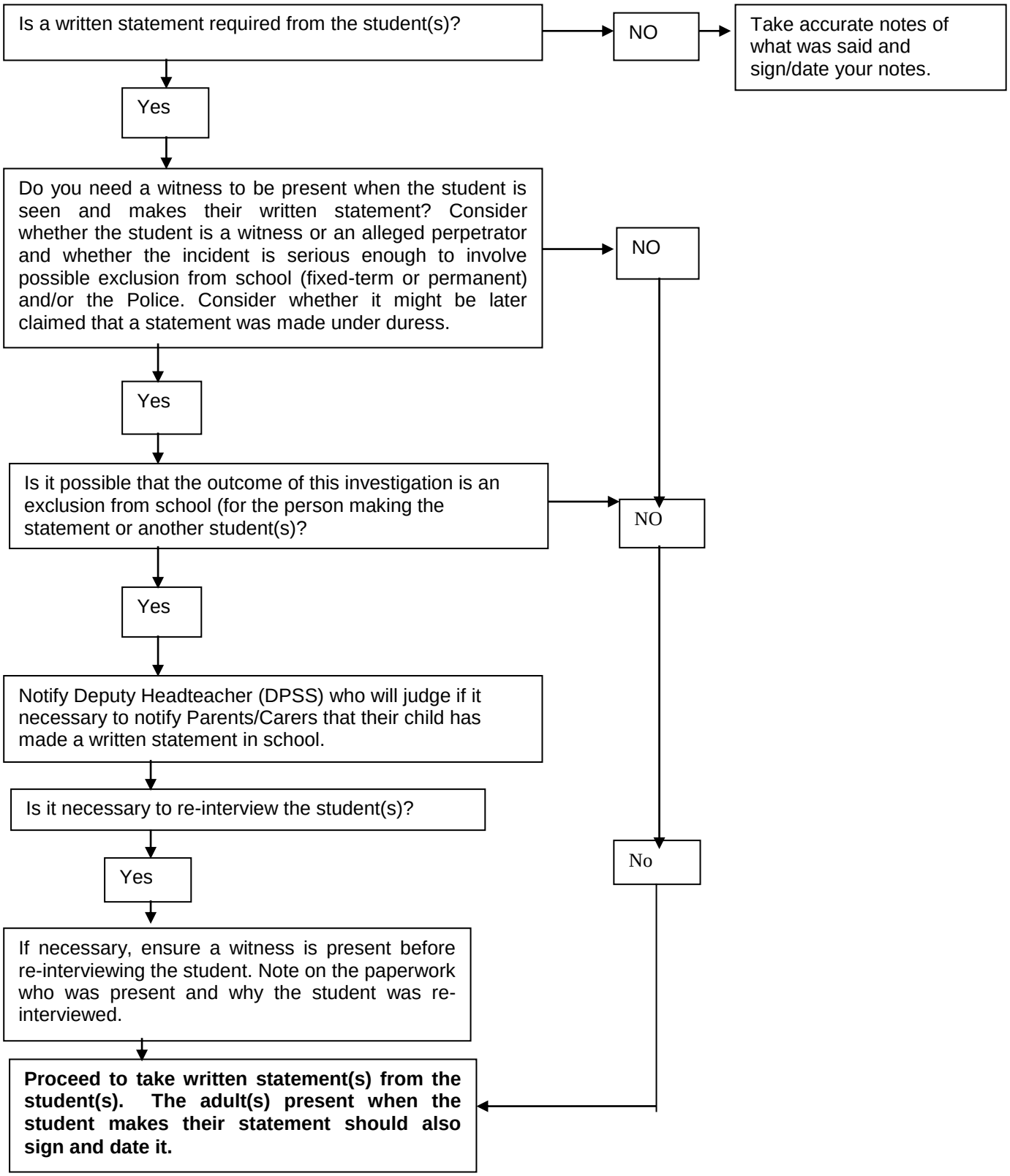


Flowchart of questions for taking statements from students

General:

This flowchart is to be read in conjunction with the Data Protection Policy. The general guidance needs to be followed:- Statements should be signed and dated, all people named in the statement should be easily identifiable (i.e., surnames must be included) and care must be taken to ensure that students cannot later claim that a statement was made under duress.

Seek advice is you are not sure about what to do at any stage and ensure that the outcome of the discussion is recorded.



Appendix 1 Links to resources and guidance

ICO Guidance for schools
http://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx
A downloadable guide for schools

Specific information for schools is available here
http://ico.org.uk/for_organisations/sector_guides/education

Specific information about use of Cloud Based technology
http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

Specific Information about CCTV
http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit
http://www.irms.org.uk/groups/public-sector/resources/134-records-management-toolkit-for-schools
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143669/handling-dbs-cert.pdf Details of storage and access to DBS certificate information.

DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Privacy Notice
Information about students in schools.

Data Protection Act 1998: How we use student information

We collect and hold personal information relating to our students and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our students' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. *For students enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.*

O*nce our students reach the age of 13, the law requires us to pass on certain information to Durham County Council who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent/guardian can request that* ***only*** *their child's name, address and date of birth be passed to Durham Count Council by informing your child's head of year.* This right is transferred to the child once he/she reaches the age 16. *For more information about services for young people, please go to our local authority website.*

We will not give information about our students to anyone without your consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please email: **enquiries@fram.durham.sch.uk**

We are required, by law, to pass some information about our students to the Department for Education (DfE). This information will, in turn, then be made available for use by Durham County Council.

The DfE may also share student level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to student level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit:
https://www.gov.uk/guidance/national-student-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) student level data has been provided to, please visit: https://www.gov.uk/government/publications/national-student-database-requests-received

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

our local authority at http://www.durham.gov.uk/dataprotection or

the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Privacy Notice
The school workforce: those employed to work, or are otherwise engaged to work, at Framwellgate School Durham

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at our Academy. This is for employment purposes to assist in the running of the Academy and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

Wendy.Pattison@fram.durham.sch.uk

Privacy Notice
Students and Staff

The Data Protection Act 1998: How we use your information in relation to CCTV, Text messaging and biometric fingerprinting

CCTV

The Academy has installed CCTV equipment for the purpose of site safety and security of our students, staff and visitors. The Academy has appropriate signage around the campus and has a protocol for the management and disposal of images held. For enquiries regarding our CCTV protocol, please email enquiries@fram.durham.sch.uk

Text Service

The Academy uses a texting service managed by "Truancy Call" and "Teachers to Parents" to communicate with parents and/or staff. This is primarily for the safety and security of our staff and students, and to share important information. Please contact enquiries@fram.durham.sch.uk for further information or if you want to opt out of this arrangement.

Biometric Data

The Academy uses a biometric system for lunch payments for students and staff. This is managed by "Cash Registers Buccleuch Limited (C.R.B.)" The use of the data complies with DFE guidance. The biometric information will be used by Framwellgate School Durham for School Meals administration (cash free system). The Academy does not store information about the actual fingerprint. Instead, this is converted into a unique reference number to administer school meals. Parents are asked to give written consent when their child starts schools. In giving consent, you are authorising the school to use your child's biometric information for this purpose until he/she either leaves the school or ceases to use the system.

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school.

Please contact enquiries@fram.durham.sch.uk for further information or if you want to opt out of this arrangement.