



RECORD OF ISSUE

ISSUE	DATE	NEXT REVIEW DATE	SUMMARY
1			Issue 1 follows a change of Headteacher
2			
3	Jan 2016	Jan 2018	Review by Head teacher and Business Manager
4	April 2018		Review in preparation for the introduction of the General Data Protection Regulation

DOCUMENT CONTROL

This document is the property of South Cumbria Pupil Referral Service and is subject to controlled issue by: South Cumbria Pupil Referral Service

	NAME	SIGNATURE	DATE
AUTHOR	L Balderstone		
CHAIR OF MANAGEMENT COMMITTEE	S Jackson		26.6.18

Contents

1. Rationale.....	1
2. Associated School Policies	1
3. Compliance	1
4. The General Data Protection Regulation, 2016.....	1
5. Responsibilities Under the GDPR and Registration.....	2
6. Definitions	2
7. Data Protection Principles.....	3
7.1 processed lawfully, fairly and in a transparent manner in relation to individuals.....	Error! Bookmark not defined.
7.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;.....	Error! Bookmark not defined.
7.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;.....	Error! Bookmark not defined.
7.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;.....	3
7.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;.....	3
7.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	3
8. Consent as a Basis for Processing	4
8.1 Fair Processing.....	5
9. Subject Access Rights (SARS).....	5
9.1 Processing Subject Access Requests.....	5
10. Authorised Disclosures.....	6
10.1 Legal Disclosure.....	6
10.2 Illegal Disclosure.....	6
11. Publication of School Information	6
11.1 Email.....	6
11.2 CCTV	7
11.3 Images/Photographs	7
12. Data Integrity.....	7
12.1 Data Accuracy	7
12.2 Data Adequacy and Relevance	7

Data Protection Policy

12.3 Length of Time	7
13. Identification of Data	7
14. Data and Computer Security.....	8
14.1 Physical Security.....	8
14.2 Logical Security	8
14.3 Procedural Security.....	8
15. Secure transfer of data and access out of school	9
16. Disposal of Data.....	9
17. Training & Awareness.....	9
18. Enquiries	9

Appendix A – Access to Personal Data Request

Appendix B – Privacy Notice - Staff

Appendix C – Privacy Notice – Pupils

Appendix D – CCTV Procedures

South Cumbria Pupil Referral Service

DATA PROTECTION POLICY

1. Rationale

The **South Cumbria Pupil Referral Service** is committed to a policy of protecting the rights and privacy of individuals, including students, staff and others, in accordance with the GDPR.

The **South Cumbria Pupil Referral Service** needs to process certain information about its staff, students and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of a student's progress
- agreeing awards
- collecting fees
- complying with legal obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation, 2016, the **South Cumbria Pupil Referral Service** must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. Associated School Policies

- Privacy Notice
- Overarching Safeguarding Statement
- Child Protection Policy
- E-Safety Policy and Acceptable Use Agreements
- Health and Safety Policy
- Behaviour & Discipline Policy

3. Compliance

This policy applies to the Management Committee, staff and students of the **South Cumbria Pupil Referral Service**. Any breach of this policy, or of the Regulation itself will be considered an offence and the school's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with the **South Cumbria Pupil Referral Service**, and who have access to personal information, will be expected to read and comply with this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

The Information Commissioner's Office (ICO) [Click here to access](#) gives further detailed guidance and the **South Cumbria Pupil Referral Service** undertakes to adopt and comply with ICO guidance.

4. The General Data Protection Regulation, 2016

This piece of legislation came into force on 27th April 2016. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a

Data Protection Policy

'subject access request' (sample held at Appendix A). Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for school students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Student Information) (England) Regulations 2000.' For more detailed information on these Regulations see the Data Protection Guide on the ICO website.

5. Responsibilities Under the DPA and Registration

The South Cumbria Pupil Referral Service will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Head teacher of the school is responsible for all day-to-day data protection matters, and s/he will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the school.

South Cumbria PRU is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. *Registration Number: ZA074022.*

Compliance with the legislation is the responsibility of all members of the school who process personal information.

Individuals who provide personal data to the school are responsible for ensuring that the information is accurate and up-to-date.

6. Definitions

Data Controller:	Any individual or organisation who controls personal data, in this instance the School.
Personal Data:	Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
Sensitive Personal Data:	Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.
Relevant Filing System:	Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records, microfiches.
Data Subject:	An individual who is the subject of the personal data, for example, employees, pupils, claimants etc.
Processing:	Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.
Accessible Records:	Any records which are kept by the Organisation as part of a statutory duty, e.g. pupil records, housing tenancy records, social services records.
Parent:	Has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

7. General Data Protection Regulation Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, the **South Cumbria Pupil Referral Service** undertakes to:

7.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

The South Cumbria Pupil Referral Service will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant. (see privacy notice)

7.2 processed lawfully, fairly and in a transparent manner in relation to individuals;

The South Cumbria Pupil Referral Service will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

7.3 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

The South Cumbria Pupil Referral Service will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

7.4 Keep personal data accurate and, where necessary, up to date

The South Cumbria Pupil Referral Service will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the school if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the school to ensure that any notification regarding the change is noted and acted on.

7.5 Only keep personal data for as long as is necessary

The South Cumbria Pupil Referral Service undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the **South Cumbria Pupil Referral Service** will undertake a regular review of the information held and implement a weeding process when, e.g. students or a member of staff leaves the school.

The South Cumbria Pupil Referral Service will dispose of any personal data in a way that protects the rights and privacy of the individual concerned. See also Section 16.

7.6 Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including:

- a right to be told the nature of the information the school holds and any parties to whom this may be disclosed;
- a right to prevent processing likely to cause damage or distress;
- a right to prevent processing for purposes of direct marketing;
- a right to be informed about the mechanics of any automated decision making process that will significantly affect them;
- a right not to have significant decisions that will affect them taken solely by automated process;
- a right to sue for compensation if they suffer damage by any contravention of the legislation;
- a right to take action to rectify, block, erase, or destroy inaccurate data;

Data Protection Policy

- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened;

The South Cumbria Pupil Referral Service will only process personal data in accordance with individuals' rights.

7.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The South Cumbria Pupil Referral Service will ensure that all personal data is accessible only to those who have a valid reason for using it.

The South Cumbria Pupil Referral Service will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access;
- keeping all personal data in a lockable room with key-controlled access;
- password protecting personal data held electronically;
- archiving personal data on disks which are then kept securely (lockable cabinet);
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not be visible except to authorised staff.

In addition, the **South Cumbria Pupil Referral Service** will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work (Currently P&W Confidential). Hard drives of redundant PCs will be wiped clean before disposal, or if that is not possible, destroyed physically (currently undertaken by Miller Waite (Curriculum Drive) and Agilisys (Council machines)).

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data.

7.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The South Cumbria Pupil Referral Service will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so the **South Cumbria Pupil Referral Service** will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the school collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. Consent as a Basis for Processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when schools are processing any sensitive data, as defined by the legislation.

The South Cumbria Pupil Referral Service understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

The South Cumbria Pupil Referral Service will ensure that any forms used to gather data on an individual will contain a statement (Privacy Notice – formerly known as Fair Processing Notice) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

The South Cumbria Pupil Referral Service will ensure that if the individual does not give her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

8.1 Fair Processing

Under the “Fair Processing” requirements in the Data Protection Act, the school will inform staff and separately parents/carers of all pupils/students of the data they hold on the staff member or pupils/students, the purposes for which the data is held and the third parties (e.g. LA, DfE, QCA, Inspira etc.) to whom it may be passed. This fair processing notice, now known as a Privacy Notice will be passed to staff when they join the school and parents/carers through *the home-school agreement*. Parents/carers of young people who are new to the school will be provided with the Privacy Notice through *the home-school agreement*.

9. Subject Access Rights (SARS)

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

Data Protection Policy

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

9.1 Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form, available from the School Office.

Completed forms should be submitted to the **Headteacher**. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (*if different*), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

10. Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

10.1 Legal Disclosure

Data Protection Policy

A “**legal disclosure**” is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

10.2 Illegal Disclosure

An “**illegal disclosure**” is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School’s registered purposes.

11. Publication of School Information

The **South Cumbria Pupil Referral Service** publishes various items which will include some personal data, e.g.

- event information
- staff information
- lists of students

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted to internal school access only. Therefore it is the **South Cumbria Pupil Referral Service’s** policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Staff records appertaining to individual staff will remain of a confidential nature between the Head teacher and the member of staff and, where appropriate, the member of staffs’ line manager.

11.1 Email

It is the policy of the **South Cumbria Pupil Referral Service** to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the school’s email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the school may be accessed by someone other than the recipient for system management and security purposes.

11.2 CCTV

There are some CCTV systems operating within the **South Cumbria Pupil Referral Service** for the purpose of protecting school members and property. The **South Cumbria Pupil Referral Service** will only process any personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

For detailed guidance on CCTV see the ICO CoP on CCTV (held in school) or which can be accessed at [Click here to access](#) and the school CCTV Procedures appended to this Policy.

11.3 Images/Photographs

Information regarding our policy for the use of pupils’ images and model Parental Consent forms can be found in CCC Safety Advice Note SAN(G)21

12. Data Integrity

The school undertakes to ensure data integrity by the following methods:

12.1 Data Accuracy

Data Protection Policy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Management Committee for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

12.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

12.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Headteacher to ensure that obsolete data are properly erased. See also Section 16.

13. Identification of Data

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject (details can be found in Section 10). Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

14. Data and Computer Security

The South Cumbria Pupil Referral Service undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

14.1 Physical Security

Appropriate building security measures are in place, door access controls, intruder alarm system. Discs, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

14.2 Logical Security

- Security software is installed on all computers containing personal data.
- 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 are only assigned access to those files which they need to access.
- All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Data Protection Policy

- 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.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
 - the data must be encrypted and password protected;
 - the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
 - the device must offer approved virus and malware checking software;
 - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. Both the local authority network and the school network are backed up and back-ups held off-site.

14.3 Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Further information can be found in the school e-Safety Policy.

Overall security policy for data is determined by the head teacher/Management Committee and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to the **headteacher** (the person responsible).

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

15. Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (NB. to carry encrypted material is illegal in some countries)

16. Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

17. Training & Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff;
- Staff meetings/briefings/Inset;
- Day to day support and guidance from the Responsible Person.

18. Enquiries

Information about the school's Data Protection Policy is available from *the head teacher*. General information about the Data Protection Act can be obtained from the Information Commissioners Office <http://www.ico.gov.uk/>.

A copy of this policy will be issued to all employees and covered in new staff Induction Training. It will be reviewed biennially, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

ACCESS TO PERSONAL DATA REQUEST
(Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer's Surname		Enquirer's Forenames	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			YES / NO
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			YES / NO
If YES,			
Name of child or children about whose personal data records you are enquiring:	<hr/> <hr/> <hr/> <hr/>		
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

We, the **South Cumbria Pupil Referral Service** are the **Data Controller** for the purposes of the Data Protection Act. Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. This personal data includes some or all of the following: identifiers such as name and National Insurance Number; characteristics such as ethnic group; employment contract and remuneration details; post "A" level qualifications; and absence information.

The collection of this information will benefit both national and local users by:

- improving the management of school workforce data across the sector;
- enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- informing the development of recruitment and retention policies;
- allowing better financial modelling and planning;
- enabling ethnicity and disability monitoring;
- supporting the work of the School Teacher Review Board and the School Support Staff Negotiating Body.

We are required to pass on some of this data to:

- the Local Authority (LA)
- the Department for Education (DfE)

If you require more information about how the Local Authority (LA) and/or DfE store and use this data please go to the following websites:

<http://www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp>

and

<http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc>

<http://www.education.gov.uk/researchandstatistics/childrenandyoungpeople/a0064391/who-the-department-passes-pupil-data-to>

Contact:

If you would like to discuss anything in this privacy notice, please contact:

Leeann Evans
Data Protection Officer
 South Cumbria Pupil Referral Service
 Newbridge House
 Ewan Close
 Barrow-in-Furness
 Cumbria
 LA13 9HU

leeann.evans@cumbria.gov.uk
 or 01229407470

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- **Performance Unit**
Children's Services
 5 Portland Square
 Carlisle
 CA1 1PU
 website: www.cumbria.gov.uk/childrensservices
 email: shaun.smith@cumbriacc.gov.uk
 Telephone: 01228 226860
- **Public Communications Unit**
Department for Education
 Sanctuary Buildings
 Great Smith Street
 London
 SW1P 3BT
 Website: www.education.gov.uk
 email: <http://www.education.gov.uk/help/contactus>
 Telephone: 0370 000 2288.

PRIVACY NOTICE – How we process pupil data

Why do we collect and use pupil information?

We collect and process pupil information under the following lawfulness of processing personal data

- Article 6a – Consent to processing data for one or more specific purpose
- Article 6c Compliance with legal obligations, which the controller is subject to
- Examples of these include obligations placed on the PRU by the DfE include (More information on these can be found at <https://www.gov.uk/education/data-collection-and-censuses-for-schools>)
 - Attendance
 - Special Educational Needs and Disabilities (SEND)
 - Progress and Attainment
- Article 6d – in order to protect the vital interests of the data subject or of a natural living person
- We also collect and process data under Article 9 – Processing of special categories of personal data
 - Where we have explicit consent
 - To protect vital interests of the data subject

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to support re-integration into another setting
- to assess and support the pupils wider needs
- to assess the effectiveness of our services
- to comply with the law regarding data sharing

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as baseline testing, strengths and difficulties)
- Relevant medical information (such as diagnosed conditions and medications)
- Special educational needs information (such as EHCP contributions / applications)
- Behavioural information (Such as behaviour Management Plans to decide how best to support pupils)
- Post 16 learning information (such as information to inform us of students progression into training, or employment)

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for no longer than needed and as specified in our retention schedule. All records are kept on site until the young person is 19 years old at which point the file is transferred to the Records management who store the record until the young person is 25 year old. This is in line with the IRMS: Information Management Toolkit for schools.

Who do we share pupil information with?

We routinely share pupil information with:

- education, training, careers and examining bodies
- school staff and boards
- Inclusion Panels
- family, associates and representatives of the person whose personal data we are processing
- local and central government
- healthcare professionals
- social and welfare organisations
- police forces and Youth Offending teams
- courts
- current, past or prospective employers

- voluntary and charitable organisations
- business associates and other professional advisers
- suppliers and service providers
- financial organisations
- security organisations
- press and the media

Aged 14+ qualifications

For pupils enrolling for post 14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications

Why we share pupil information

- We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
- We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
- We are required to pass information about our pupils to the Department for Education (DfE) under regulation 4 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Youth support services

What is different about pupils aged 13+?

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent

controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and 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 pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact (see below)

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- withdraw consent
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Contact:

If you would like to discuss anything in this privacy notice, please contact:

Leeann Evans
Data Protection Officer
South Cumbria Pupil Referral Service
Newbridge House
Ewan Close
Barrow-in-Furness
Cumbria
LA13 9HU

leeann.evans@cumbria.gov.uk
or 01229407470

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- **Performance Unit**
Children's Services
5 Portland Square
Carlisle
CA1 1PU
website: www.cumbria.gov.uk/childrensservices
email: shaun.smith@cumbriacc.gov.uk
Telephone:: 01228 226860
- **Public Communications Unit**
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk
email: <http://www.education.gov.uk/help/contactus>
Telephone: 0370 000 2288

CCTV Procedures

South Cumbria Pupil Referral Service

1. Introduction

“The purpose of this policy is to regulate the use of Close Circuit Television and its associated technology in the monitoring of both the internal and external environs of South Cumbria Pupil Referral Unit” (hereafter referred to as ‘the school’)

CCTVs are installed internally and externally in the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

This policy applies to all personnel, and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of recorded materials

- The system comprises a number of fixed and dome cameras located around the school site. All cameras are monitored from a Central Control Room and are only available to selected senior staff on the Administrative Network
- This Code follows Data Protection Act guidelines.
- The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.
- The CCTV system is owned by the school.

2. Objectives of the CCTV scheme

- To protect the school buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the school

3. Statement of intent

- The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.
- The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.
- Cameras will be used to monitor activities within the school and its grounds and to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the school, together with its visitors.
- Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.
- Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the school's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

- Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.
- The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the school CCTV.
- Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. monitoring of political or religious activities, or employee and/or pupil evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives.
- CCTV monitoring of public areas, for security purposes, will be conducted in a manner consistent with all existing policies adopted by the school including Discrimination, Bullying and Harassment, Sexual Harassment etc.
- The code of practice for video monitoring prohibits monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc.
- The system is in place to monitor suspicious behaviour and not individual characteristics
- Video monitoring of public areas, for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law
- The head teacher will approve the temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. (Temporary cameras does not include mobile video equipment or hidden surveillance cameras used for criminal investigations)
- Consideration will be given to both staff and pupils regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment
- The Head teacher will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- The camera control will be monitored to ensure it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas
- When a zoom facility on a camera is being used, a second person will be present with the camera operator to guarantee that there is no unwarranted invasion of privacy

4. Operation of the system

- The Scheme will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.
- The day-to-day management will be the responsibility of both the Senior Leadership Team and the Office Team during the day.
- The CCTV system will be operated 24 hours each day, every day of the year.

5. Control Room (Main Office)

- The Business Manager will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.
- Unless an immediate response to events is required, and authorised by the headteacher and staff in the CCTV Control Room must not direct cameras at an individual or a specific group of individuals.

- Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below.
- Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be in the centre's signing in book. The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the headteacher, and must be accompanied by her throughout the visit.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- If out of hours emergency maintenance arises, the Control Room Operators must be satisfied of the identity and purpose of contractors before allowing entry.
- A visitors book will be maintained in the centre. Full details of visitors including time/data of entry and exit will be recorded.
- Outside of school hours the office must remain secured
- Other administrative functions will include maintaining video Data and hard disc space, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Liaison

Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring Procedures

- Camera surveillance may be maintained at all times.
- A monitor is installed in the Main Office to which pictures will be continuously recorded.

8. Disc Procedures

- In order to maintain and preserve the integrity of the Data used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
 - Each disc must be identified by a unique mark.
 - Before using each disc must be cleaned of any previous recording.
 - The controller shall register the date and time of tape insert, including disc reference.
 - A disc required for evidential purposes must be sealed, witnessed, signed by the controller, dated and
 - stored in a separate, secure, evidence disc store. If a tape is not copied for the police before it is sealed, a
 - copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller,
 - dated and returned to the evidence disc store.
 - If the disc is archived the reference must be noted.
- Data may be viewed by the Police for the prevention and detection of crime, authorised officers of Cumbria County Council for supervisory purposes, authorised demonstration and training.
- A record will be maintained of the release of Data to the Police or other authorised applicants. A register will be available for this purpose.
- Viewing of Data by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.
- Should a tape/disc be required as evidence, a copy may be released to the Police under the procedures described previously in this Code. Data will only be released to the Police on the

clear understanding that the disc remains the property of the school, and both the disc and information contained on it are to be treated in accordance with his code. The school also retains the right to refuse permission for the Police to pass to any other person the disc or any part of the information contained thereon. On occasions when a Court requires the release of an original disc this will be produced from the secure evidence tape store, complete in its sealed bag.

- The Police may require the school to retain the stored Data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Headteacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9. Breaches of the code (including breaches of security)

- Any breach of the Code of Practice by school staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action.
- Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.
- Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school, or a pupil

10. Assessment of the scheme and code of practice

- Performance monitoring, including random operating checks, may be carried out by the Business Manager & contractors maintaining the system.

11. Complaints

- Any complaints about the school's CCTV system should be addressed to the Headteacher.
- Complaints will be investigated in accordance with Section 9 of this Code.

12. Access by the Data Subject

- The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.
- Requests for Data Subject Access should be made on an application form available from the Headteacher.

13. Public information

- Copies of this Code of Practice will be available to the public from the Main Office.

Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the school.
- The Control room will not be manned out of school hours.
- The Control Room is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- Recording Data will be used properly indexed, stored and destroyed after appropriate use.
- Data may only be viewed by Authorised School Officers, Control Room staff and the Police.

- Data required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Data will not be made available to the media for commercial or entertainment.
- Data will be disposed of securely by incineration.
- Any breaches of this code will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Headteacher.