



DATA PROTECTION POLICY

Ratified by Governors/Principal:	Principal
Current ratification date:	Summer 2015
Review frequency:	Annually
Next review date:	Summer 2016
Responsibility of:	June Foxtton

STATEMENT OF POLICY

The Academy needs to collect and use certain types of information about students, their families, employees and with whom it deals, in order to perform its functions. This includes information on current, past and perspective employees, students, persons with parental responsibility, suppliers, customers, service users and others with whom it communicates. The Academy is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of Government.

POLICY AIMS

- This policy outlines the Academy's arrangements to access personal information by students, persons with parental responsibility, public and employees in accordance with the Data Protection Act 1998 [DPA].
- This policy will be communicated to all employees and will be published to employees through the Academy's normal channels.
- The policy applies to all personal information held by the Academy irrespective of ownership. Personal Information is defined for the purposes of this policy as being any information which an individual can be identified [including computer storage, documents, photographs, CCTV images, and voice.]

SCOPE

- The policy also applies to all contractors and agencies operating on behalf of the Academy or in the Academy premises. For the purpose of this policy the term "employee " covers all of these groups.

POLICY OBJECTIVES

- This policy outlines the Academy's approach to ensuring all employees effectively process and manage personal information within set standards, to protect the privacy of individuals and to comply with the principles and requirements of the DPA and other legislation. It informs employees on procedures which comply with the DPA when handling personal information about students, parents, visitors, clients, contractors and employees.
- This policy should be complied with for personal information relating to all individuals, deceased or living.
- This policy should be read in conjunction with the E-safeguarding Policy and the Redcar and Cleveland Borough Council Privacy Notice, APPENDIX A.
- The policy and guidelines cover requests for information from individuals for their own personal data. Such requests, defined as subject access requests [SARs], should be handled in accordance with this policy, in compliance with the Data Protection Act 1998. A definition of terms is available in Appendix B
- To promote the effective, consistent and legal processing of personal information by defining a personal information handling policy
- To ensure that all employees are aware of the consequences of misuse or abuse of personal information
- To establish and maintain trust and confidence in the Academy's ability to process personal information
- To ensure compliance with legislation, guidance and standards relating to the handling of personal information

MONITORING AND REVIEW

- The policy and guidelines will be reviewed annually to take into account changes in legislation and to ensure they remain timely and relevant. Any changes will be publicised through the Information Commissioners Office [ICO] and normal communication channels.
- The effectiveness of the policy will be assessed through the monitoring of requests for personal information, the Academy's response to these, and complaints. These events will be collated into an annual report. Where issues of concern arise, then the ISO and IGT will be approached.
- The policy will be published on the Academy's website and hard copies published upon request.
- An information audit will be conducted every three years by the Academy's administration team and Network Manager and any recommendations complied with, within agreed timescales. This also complies with Section 46 of the Freedom of Information Act.

PROCEDURE

- The Academy regards the lawful and correct treatment of personal information as critical to successful operations and to maintaining confidence between those with whom it deals. It is essential that it treats personal information lawfully and correctly.
- The purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals. It regulates the processing of personal information including obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal information and gives rights to those whose information is being processed.

PROCESSING PERSONAL INFORMATION

- The processing of personal information is defined as encompassing everything that we do with personal information including the sharing, transferring or disclosing of personal information to another organisation or internally.
- Personal Information must be processed in accordance with the **eight principles** under the Data Protection Act 1998 unless an exemption applies. [APPENDIX C: Data Protection Act 1998: Eight Principles]
- Employees must respect personal information that they have access to and treat it in the manner in which they would expect their personal details to be treated
- Employees must have regard and respect for the privacy of students, persons with parental responsibility and employees and process their personal information accordingly
- Access to personal information should be deleted and disposed of in line with the Data Retention Procedure
- Personal Data will be held securely and accessible only by those with a need and right to know. The Principal is responsible for ensuring that personal information is surrounded by appropriate security, i.e. relevant to the sensitivity of the personal information being processed.
- Arrangements and contingencies need to be in place in order to protect personal information from loss due to natural and unnatural disaster e.g. flood, arson, theft

- Personal information must not be transmitted or transported externally via manual or electronic means without appropriate security. Portable devices including laptops, CDs, DVD, USB memory sticks, which contain personal information, will use encryption to protect against losses or access by unauthorised persons. The Department for Education (DfE) requests that no identifiable COLLECT information be accessed by laptop unless it is encrypted. This is because COLLECT data is the responsibility of the DfE. Any laptop containing sensitive data could be lost or could be seen by unauthorised people in the laptop is used outside the Academy
- Personal information must be disposed of safely and securely when it has reached the end of its shelf life
- Personal information will not be passed on to any third party unless any one or more of the following apply [Schedules 2 and 3 of the Data Protection Act]:
 - ❖ permission or consent is obtained
 - ❖ the organisation requesting the information has a legal right to the information [e.g. police investigating a crime]
 - ❖ it is a requirement of law
 - ❖ it is to comply with a court order
 - ❖ it is necessary to provide educational services
 - ❖ the Academy believes it is in the subject's own interest
 - ❖ the Academy believes it is in the overall public interest and in a particular instance this is judged to outweigh the other considerations
- At the point of collection the data subject will be informed of the purposes for which the information is being collected and processed together with any other relevant details regarding this processing. At this time, where choices are available the child/young person or persons with parental responsibility will be given the opportunity to opt out of the Academy's non-statutory information processing arrangements, e.g. consent to the taking of images for publicity purposes
- The Academy will promote good practice in the sharing of information with its partners, Government agencies and departments and other public and private sector organisations. All sharing will comply with the Data Protection Act 1998 and the current General Information Sharing Protocol [GISP]
- The quality and accuracy of personal information should be relevant to the purpose for which it is to be used
- The purpose for which personal information is processed in the Academy will be detailed in the school Data Protection Notification which will be renewed annually with the Information Commissioner's Office who will submit amendments as required
- Processing of information for a purpose not reflected in the Data Protection Act 1998 or in the notification must be approved by the ISO or IGT
- Any inaccurate or misleading information will be checked and corrected as soon as the student or parent brings this to the Academy's attention
- The rights of data subjects as defined by the Data Protection Act 1998, and specifically their right of access to their own personal information will be complied with fully and given appropriate respect and priority

THE SUBJECT ACCESS REQUEST PROCEDURE

- Requests by individuals [or their representative] for copies of their own information **must be in writing** and supported by significant proof of identity. The following originals, [not photocopies] are suggested:
 - ❖ Passport
 - ❖ Driving license; or
 - ❖ Birth/marriage certificate
- The need to check and verify the identity of the requester can be particularly important where the person is a child or someone is purportedly making the request on behalf or in respect of a child
- Enquirers should be provided with a Subject Access Request Form
- The decision on whether to release information in the event of a request will be that of the Principal. This is also to ensure compliance within timescales
- The information must not be deleted or disposed of, after the receipt of a request, unless requested by the subject. Subjects have a right to have incorrect or inaccurate information corrected
- Subject Access Requests will be supplied within **15 school days for students and 40 days for employees**. Where an investigation of a member of staff has commenced and Subject Access has been requested by that member of staff, the processing of the request should be undertaken as quickly as possible. In the event that the complaint is received regarding a Subject Access Request, the complaint will be addressed following the Academy's Complaints Procedure. Records of proceedings and decisions made will be kept in order to provide evidence for any external review of the complaint by the Information Commissioner's Office
- Requests for personal information held by the Academy about an individual may result in the Academy seeking clarification from the requestor, for example to specify an area of information required, services or timescales. In cases where clarification is sought, the clock stops until clarification is received and then restarts from where it left off.

TRAINING

- Training on the Data Protection Act 1998 and personal information handling is required by all staff. New staff will also require training during induction. Training is seen as one measure to help maintain compliance with the Data Protection Act
- Inappropriate and Unacceptable Use [see E-safeguarding Policy]
- Unacceptable use includes:
 - ❖ unauthorised access to personal information
 - ❖ unauthorised disclosure of personal information
 - ❖ unauthorised use of person information, e.g. use of which the data subject has not been informed/consented to [as in Section 2 and 3 of the Data Protection Act 1998 and the Fair Processing Notice]; and
 - ❖ non-adherence to the Academy's policies and local authority's information sharing protocols

- Employee, student or client personal information must not be used for:
 - ❖ any illegal purpose
 - ❖ any purpose which is inappropriate in the workplace virtue of the fact it may cause embarrassment or distress to another person or may bring the Academy into disrepute; or
 - ❖ any purpose which is not in accordance with the employee's role or job description
[This is not an exhaustive list]
- Employees are required to notify the Principal, if they become aware or suspect that personal information is being misused or handled inappropriately

NON-COMPLIANCE WITH LEGISLATION AND POLICY

- The Principal is responsible for ensuring that employees' responses to requests for personal information remain appropriate and are in accordance with this policy and the Data Protection Act 1998
- The Principal must ensure that instructions they give to employees, relating to requests for personal information and the processing of personal information comply with legislation and Academy policy
- Employees need to be aware that arrangements need to be in place that avoid parental and visitor contact with personal information to which they do not have a right
- All employees must be aware of their own obligations with regard to the disclosure and the processing of personal information
- Employees not complying with this policy or legislation will have matters reviewed and may be dealt with under the Academy's Disciplinary Procedure. In the event of non-compliance by an agency worker, casual worker or contractor, his/her work with the Academy will also be reviewed under the Academy's Disciplinary Procedure, depending on the circumstances of the case.



PRIVACY NOTICE

For Pupils in Schools, Alternative Provision and Pupil Referral Units

Privacy Notice - Data Protection Act 1998

Freebrough Academy are a data controller for the purposes of the Data Protection Act. We collect and receive information from you, your child's previous school and the Learning Records Service. We hold this personal data and use it to:

- Support teaching and learning
- Monitor and report student progress
- Provide appropriate pastoral care
- Assess the school's process

This information includes contact details, national curriculum assessment results, attendance information¹ and personal characteristics, such as the student's ethnic group, any special educational needs and relevant medical information. A unique learning number (ULN) will be provided by the Learning Records Service if your child is enrolling for post 14 qualifications. This will be provided by the Learning Records Service, which can also provide details of the learning or qualifications your child has undertaken.

In addition for Secondary and Middle deemed Secondary Schools

Once your child is aged 13 or over, the law requires us to pass on certain information to the provider of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide the address of your child, their date of birth and any further relevant information to support the services' role.

However, if your child is age 16 or over, you and your child can ask that no information beyond names, addresses and your child's date of birth be passed to the support service. This right transfers to your child on their 16th birthday. You or your child will need to inform the Academy to opt out of this arrangement. For more information about young people's services, please go to the National Careers Service page at

<https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx>

We will not give information about your child to anyone outside the Academy without their, or your consent unless the law and our rules allow us to.

¹ Attendance information is **NOT** collected as part of the Censuses for the Department for Education for the following pupils / children - a) in Nursery schools; b) aged under 4 years in Maintained schools; c) in Alternative Provision; and d) in Early Years Settings. This footnote can be removed where Local Authorities collect such attendance information for their own specific purposes.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use of the Local Authority.

If you want to see a copy of the information about you or your child that we hold and/or share, please contact the Academy.

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

- <http://www.redcar-cleveland.gov.uk/rcbcweb.nsf/Web+Full+List/11DAE1479E0981EC802574E90053BF6D?OpenDocument>
- <http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause>

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:

- Redcar & Cleveland Borough Council
People Services
Children & Young People Team
Seafield House
Kirkleatham Street
REDCAR
TS10 1RT

Website: www.redcar-cleveland.gov.uk/Enquiries

Email: CYPTeam@redcar-cleveland.gov.uk

Tel: (01642) 771161 or (01642) 444369

- 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>

Tel: 0370 000 2288

DEFINITIONS

[a]	<p>Personal Information Information relating to an individual who can be identified from the information or from other information in possession of the organisation. This is information that affects a person's privacy whether in their personal or family life, business or professional capacity and included the name, address and telephone number of an individual. It will also include information on a person's medical history, an individual's salary details and includes expression of opinion about the individual and of the intentions of the organisation in respect of that individual. Personal information also includes CCTV images and photographs which enable the identification of an individual.</p>
[b]	<p>Personal Sensitive Information As defined in the Act as racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal convictions.</p>
[c]	<p>Data Subject Any living individual who is the subject of personal information held by an organisation, e.g. pupil, parent, member of Academy staff, council employee, agency worker, casual worker, client, member of the public, partnership worker.</p>
[d]	<p>Processing Any operation relating to information including: organising, retrieving, disclosing or otherwise making information available, deleting, obtaining, recording, alerting, adding to, or merging.</p>
[e]	<p>Third Party Any individual or organisation other than the information subject, the information controller or its employees or agents.</p>

Personal data is defined by the Data Protection Act as “Data relating to a living individual who can be identified from the data”. The Act gives eight principles to bear in mind when dealing with information. Data must:

1. Be processed fairly and lawfully
2. Be collected for a specified purpose and not used for anything incompatible with that purpose
3. Be adequate, relevant and not excessive
4. Be accurate and up- to- date
5. Not be kept longer than necessary
6. Be processed in accordance with the rights of the data subject
7. Be kept securely
8. Not be transferred outside the EEA [European Economic Area] unless the country offers adequate protection.