DATA PROTECTION POLICY

Document Management:	
Date Policy Approved:	29 April 2015
Date Amended:	April 2017
Next Review Date:	April 2018 to comply with the new General Data Protection Regulations
Version:	2
Approving Body:	Resources Committee

1. Introduction

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from that data. Personal data includes (but is not limited to) an individual's, name, address, date of birth, bank details and other information that identifies them. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The Trust collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3. The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

- Data must be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specific and lawful purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Personal data shall be accurate and where necessary kept up to date.
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country outside the EEA (European Economic Area), unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Responsibilities

The Trust and its Schools must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.

The Trust has a legal responsibility to comply with the Act. The Trust, as a corporate body, is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The Trust is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link:
ICO Register of Data Controllers

Every member of staff that holds personal information has to comply with the Act when managing that information.

The Trust is committed to maintaining the eight principles at all times. This means that the Trust will:

- Inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice (see **Appendix 1 & 2**)

- Check the quality and accuracy of the information held

- Apply records management procedures to ensure that information is not held longer than is necessary

- Ensure that when information is authorised for disposal it is done so appropriately

- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

- Only share personal information with others when it is necessary and legally appropriate to do so

- Set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act

- Appraise staff so that they are aware of their responsibilities and of the Trusts relevant policies and procedures

5. Subject Access / Subject Information Requests (SAR)

Any person whose details are held/processed by the school (data subjects) have a general right to receive a copy of their own information. There are a few exceptions to this rule, such as data held for child protection or crime detection/prevention purposes. ICO Data Protection Act 1988 Exemptions

The Trust will respond in writing to requests for access to pupil educational records within 15 school days. The statutory definition of an 'education record' has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of the school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil will form part of the pupil's educational record. However, it is possible that some of the information could fall outside the educational record e.g. information about the pupil provided by the parent of another child is not part of the educational record.

If the SAR does not relate to any information that forms part of the educational record, then the usual 40-day time limit as prescribed by the Data Protection Act will apply. The Trust may make a charge of up to £10 for responding to a subject access request and up to £50 (on a sliding scale for photocopying charges) for access to a pupil's educational record. A copy of the scale of charges is set out below:

Number of pages of information supplied	Maximum fee
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-59	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

The time limit for responding to a SAR does not start until the fee has been received. If a fee is payable but has not been sent with the request, you should contact the individual promptly and inform them that they need to pay

The Trust's policy for dealing with requests for subject access in respect of a pupil is as follows:

1. Requests from parents / legal guardians in respect of their own child will, provided that the child does not understand the nature of the subject access requests, be processed as requests made on behalf of the data subject (child)
2. Requests from pupils who do not understand the nature of the request will referred to the child's parents.

3. Requests from pupils who demonstrate an understanding of the request will be processed as any subject access request as outlined below:

    i. The Headteacher/Head of School (or authorised person acting on his/her behalf) will make the judgment about whether a child has the necessary level of understanding, and will seek guidance from the Data Protection Officer in the event of a dispute. See **Appendix 3** for more detail
    ii. A subject access / information request, although not compulsory, should be submitted on the appropriate forms wherever possible to ensure that the school has the required information to be able to conduct the data search and fulfil the request (**Appendix 4**). The person making the request should be made aware that this is not compulsory and it must not be used as a way of extending the 40-day time limit for responding.
    iii. Where information is not available from the Trust but is processed by another organisation, for example, the Local Authority, the requests will be directed to that organisation.
    iv. In some cases, especially with requests not submitted on the appropriate forms, further information may be required from the requester which may delay the start of the 40 day maximum period.
    v. Repeat requests will be fulfilled unless deemed unreasonable, such as second request received so soon after the first that it would be impossible for the details to have changed.

6. Complaints and Appeals
Complaints, disputes or challenges as described above should be first taken up with the Headteacher/Head of School (Data controller) or an authorised person acting on his/her behalf in the first instance.

7. Protection of Biometric Information of Children in Schools
Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with the Data Protection Act 1998.

8. Key points in relation to Biometric data:
The Trust will ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.

The written consent of at least one parent must be obtained before the data is taken from the child and used. This applies to all pupils under the age of 18. In no circumstances can a child's biometric data be processed without written consent.

The Trust will not process the biometric data of a pupil (under 18 years of age) where:

1. The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

2. No parent has consented in writing to the processing; or
3. A parent has objected in writing to such processing, even if another parent has given written consent.

The Trust will provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

9. Cloud (Educational Apps) Software Services and the Data Protection Act 1998

The key areas that the Trust is required to address in respect to Cloud services under the Data Protection Act (DPA) are:

- Compliance with overarching legal requirements
- Data processing
- Data confidentiality
- Data integrity
- Service availability
- Data transfers beyond the European Economic Area (EEA)
- Use of advertising

The Trust has a duty to explain to staff and pupils what personal data would be collected, how it will be used and by whom, and what control they have over the use of their data in this way.

Supplier compliance checklists

The supplier's checklist statements can be found here. Please click on the relevant supplier hyperlink:

• Google

• Microsoft

10. Record Management

The Trust has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time. Please find the link below that provides further information on data retention recommendations:

Record Management for School (C.f page 34-51)

11. Staff Awareness

Staff are made aware of the Data Protection Act 1998 through this policy and also posters located around the Trust named Data protection Act Do's and Don'ts (**Appendix 2**).

12. Policy Review

The Trust will review this policy in April 2018 to ensure compliance with the new General Data Protection Regulations that will come into force on 25 May 2018. They will be reviewed every two years thereafter.

Conclusion
Compliance with the 1998 Act is the responsibility of all members of the Trust. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution. This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Appendix 1

Privacy Notice - Data Protection Act 1998: How we use pupil information

Carmel Education Trust (of which Carmel College is part of) is the data controller for the purposes of the Data Protection Act. We collect and hold personal information relating to our pupils and may receive information about them from their previous school and the Learning Records Service. We hold this personal data to:

- Support our pupils learning;
- Monitor and report on their progress;
- Provide appropriate pastoral care, and
- Assess how well we are doing.

The information we hold includes 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 the may have and relevant medical information. For pupils enrolling for post 14 qualifications the Learning Records Service will give us a unique learner number (ULN) and may also give us details about their learning or qualifications.

Once our pupils are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area 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 the provider of Youth Support Services in your area by informing **Jennifer Moorhouse, College Business Manager.** This right is transferred to the child once he/she reaches the age 16. 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 you to anyone without your consent unless the law and our policies allow us to. If you want to receive a copy of the information about you that we hold or share, please contact Jennifer Moorhouse at the College - JMoorhouse@carmel.org.uk Tel 01325 523407

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 Darlington Local Authority (LA).

DfE may also share pupil 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 pupil 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-pupil-database-apply-for-a-data-extract

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

If you need more information about how the LA and DfE collect and use your information, then please go to the following websites:

- http://www.darlington.gov.uk/your-council/data-protection-and-freedom-of-information/privacy-notice/

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

Appendix 2

Privacy Notice - Data Protection Act 1998

Carmel Education Trust is the Data Controller for the purposes of the Data Protection Act.

Personal data is held and processed by the Trust and its Schools about those employed or otherwise engaged to work at the Trust. This is for employment purposes to assist in the smooth running of the Trust/School and/or enable individuals to be paid. 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;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body

This personal data includes identifiers such as name and National Insurance number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not share information about you to anyone outside the Trust without your consent unless the law allow us to.

We are required by law to pass on some of this data to the Department for Education (DfE). If you require more information about how the DfE stores and uses this data please go to the following website: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Appendix 3

Requests for information about children

Even if a child is too young to understand the implications of subject access rights, data about them it is still their personal data and does not belong to anyone else, such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so.

When considering borderline cases, you should take into account, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information
- any views the child or young person has on whether their parents should have access to information about them.

Appendix 4

Subject Access Request Form

Data Protection Act 1998

Part 1 - Person that the information relates to (the data subject).			
Title	Mr Mrs Miss Ms Other:		
Surname		Forenames	
Maiden Name / Former Names			
Date of Birth		Sex	Male Female
Current Address			
Postcode		Telephone No.	
I enclose a copy of one of the following as proof of the identity of the data subject: ☐ Birth Certificate ☐ Driving Licence ☐ Passport If none of these are available please contact the Data Protection Officer for advice on other acceptable forms of identification.			
Part 2 - Is the requested information about you (are you the data subject)?			
No the information is not about me *(go to part 3)* **Yes the information is about me** *(go to part 4)*			
Part 3 - Person (agent) acting on behalf of the data subject.			
Title	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Other:		
Surname		Forenames	
Address			
Postcode		Telephone No.	
What is your relationship to the data subject *(e.g. parent, carer, legal representative)*			
Do you have legal authority to request the data subjects Information?	Yes ☐ No ☐		
If the data subject is under 16, do you have parental responsibility for them?	Yes ☐ No ☐		

Provide proof that you are legally authorised to act on the data subjects behalf in the form of: ☐ Letter of Authority ☐ Lasting Power of Attorney ☐ Evidence of parental responsibility Other *(give details)*
Provide proof that you are the person authorised to act on behalf of the data subject by enclosing a copy of one of the following: ☐ Birth Certificate ☐ Driving Licence ☐ Passport If none of these are available please contact your Data Protection Officer for advice on other acceptable forms of identification.

Part 4 - Details of Information being requested.		
As to help us deal with your request quickly and efficiently by giving as much detail as possible about the information you want. If possible restrict your request to a particular service, period of time or incident. If necessary continue this section on a separate page.		
Information Requested:		
Information requested covers	From:	To:
Relevant details to help us locate the information. *(Address at the time, service or department, names of previous contacts etc.)*		

Part 5 - Access to the information.	
By law, the Trust is permitted to charge a minimum fee of £10 (maximum £50). This request will not be valid until payment is received.	
Do you wish to:	☐ View the information ☐ Be provided with a copy
Copies *(if requested)* **to be:**	☐ Sent to the data subject ☐ Sent to you ☐ Collected
Do you have any special needs when viewing the information or in what format it is provided?	

Part 6 - Declaration
I certify that the information provided on this form is true. I understand that the Trust is obliged to confirm proof of identity / authority and that it may be necessary to obtain further information in order to comply with this subject access request.

Name			
Signature		Date	

Warning - a person who unlawfully obtains or attempts to obtain personal information is guilty of a criminal offence and is liable to prosecution.

Part 7 - Before submitting this form please check that you have:

- ☐ Enclosed proof of the identity of the person the information is about (the data subject)? *(see part 1)*
- ☐ Enclosed proof of authority to act on behalf of the data subject? *(see part 3)*
- ☐ Enclosed proof of your identity if acting on behalf of the data subject? *(see part 3)*
- ☐ Given enough details for us to locate the information you want? *(see part 4)*
- ☐ Enclosed the £10 fee? *(see part 5)*
- ☐ Signed and dated the declaration? *(see part 6)*
- ☐ Completed all sections? *(part 3 only to be completed by a person acting on behalf of data subject)*

Please submit this form and accompanying documents by post to:

Data Protection Officer
Carmel Education Trust
Carmel College
The Headlands
Darlington
County Durham
DL3 8RW

Telephone: 01325 254525
Fax: 01325 254335

Appendix 2

Data Protection Act – Dos and Don'ts

DO

- Remember the Data Protection Act applies to personal information held in paper files, as well as to information held electronically, video, audiotapes and photographs.
- Be very careful about sensitive data concerning: race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences.
- Treat personal data held about individuals as though it were held about you
- Obtain permission from data subject to hold their personal data unless consent is obviously implied.
- Be open and tell people you hold personal data about them and why.
- Hold personal data about people only when necessary.
- Ensure personal data is kept accurate and up to date.
- Ensure that you have a contract (data processing agreement) in place when sharing personal data with other organisations.
- Be extremely careful about passing personal data to third parties (seek advice if unsure).
- Respect confidentiality and the rights of the data subject.
- Refuse requests from family or friends for information about a student or colleague, unless prior written permission has been received from the student.
- Ensure that all personal data is kept secure, not only from unauthorised access, but from fire and other hazards. Apply password protection to computers, tablets, screensavers and documents. Where possible keep your office door locked and your desk clear of personal data when you are absent and lock computers.
- Ensure all personal data is disposed of as confidential waste.
- When writing documents and emails, even informally, bear in mind that the data subject has a right to see information relating to them.
- Be vigilant if undertaking work off-site using personal data (e.g. research data, reference requests or examination scripts/results).
- Where possible, anonymise personal data for research purposes.
- Use appropriate measures for disposal of confidential information.
- Report immediately any accidental or deliberate release of personal information to the Data Protection Officer.

DON'T

- Disclose any information (including giving references) about an individual to an external organisation without first checking that the individual consents to such disclosure, or, in the case of the police, checking with the Data Protection Officer.
- Disclose any personal data over the telephone.
- Hold sensitive data about a person without explicit consent or advice from the Data Protection Officer.
- Put personal data about an individual on the Internet or in social media without their permission, unless it is a condition of their employment as a member of staff or enrolment as a student.
- Send personal data outside the European Economic Area without taking advice from the Data Protection Officer.
- Leave personal data insecure in any way, whether it is physical files or information held electronically.
- Take personal data home without particular care for security.
- Process personal data on a computer not owned or supplied by the Trust.
- Dispose of Trust computers without advice on the deletion of data from the IOC.
- Use email for sending confidential communications or unencrypted personal data, as it is relatively insecure.
- Use personal data held for one purpose for a different purpose without permission from the data subject.
- Write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. You must assume that anything that you write about a person, even in informal e-mails, may be seen by that person.
- Under any circumstances, erase or alter data following the receipt of a Subject Access Request.