# General Data Protection Regulation Policy

**Written:** May 2018
**(or to meet new legislation and practices)**

Document Control:

| Person Drafting document: | Version: | Authorised by: | On: |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## Aims

Coast Academies is committed to a policy of protecting the rights and privacy of all individuals, including pupils, staff and others, in accordance with the General Data Protection Regulation (GDPR) 2016 and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance CCTV cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

## Introduction

Coast Academies is an academy chain of three schools. Each individual academy needs to process information relating to their staff, pupils and third parties who it has a legitimate need to process information on behalf of the Coast Academies, this includes:

- Recruitment and payment of staff
- Administration of study programmes
- Recording of student progress
- Agreeing and validating examination award boards
- Collecting fees
- Compliance with legal obligations to share information with governmental bodies such as the Department for Education.

To comply with its legal obligations, specifically the GDPR (2016), Coast Academies must ensure that all personal data is collected, used and stored securely in adherence with the appropriate retention periods and not disclosed to any organisation or person without legitimate consent or an appropriate legal basis.

This policy will set out how Coast Academies and its staff will fulfil its legal obligations under GDPR (2016) and give staff appropriate guidance on what is required when dealing with information governance concerns.

## The data controller

Coast Academies processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Coast Academies is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## Compliance

Under GDPR, all organisations holding personal data are required to register as a data controller with the Information Commissioner's office. This registration permits the organisation to process information to:

- Provide education;
- Training;

- Welfare and education support services;
- Administration of school property;
- Maintaining school accounts and records;
- Undertaking fundraising;
- Support and managing our employees; and
- The use of CCTV for security and the prevention and detection of crime.

This is updated every two years to ensure that Coast Academies' activities are accurately represented.

A further requirement of GDPR is the appointment of a Data Protection Officer who will have overall responsibility for the implementation and monitoring of this policy. The schools data protection officer can be contacted at dataprotection@coastacademies.org.uk

**Roles and Responsibilities**

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf.

Whilst the Chief Executive Officer of Coast Academies has overall responsibility for Data Protection, delegated responsibility is given to the Data Protection Officer who will ensure that there is compliance with this policy and the reporting of all breaches and suspected breaches of data and near misses in accordance with the incident reporting procedure. This includes reporting information incidents to the Information Commissioner in line with the GDPR requirements. The Data Protection Officer will ensure that all correspondence and disclosures to the Information Commissioner's Office (ICO) including the Data Protection Notice and registration are kept up to date and accurate.

All staff (permanent, temporary and contracted) and contractors are responsible for ensuring that they are aware of the requirements of this policy and to ensure that all data remains adequate for its purpose and is up to date. All staff must ensure that they adhere to the principles of the GDPR and report all data breaches.

**Training and awareness**

Coast Academies' Data Protection Officer will work with the senior leaders and IT Manager to ensure that appropriate training is part of any induction process and additional training is provided to all staff to ensure that the organisation remains compliant with the appropriate legislation such as GDPR.

The DPO will also produce guidelines for staff and parents/guardians on general data protection. This will ensure that all are up to date and aware of their obligations.

**Confidentiality**

**The General Data Protection Regulation (2016) - GDPR**

This legislation came into force on 25th May 2018 and seeks to strengthen the previous legislation - the Data Protection Act (1998). Both the regulation and acts seek to regulate the use of personally identifiable data and protects the rights of all living individuals. Personal data is information which relates to any individual and may be recorded in hard (paperwork) or soft (electronic) formats, this data may include specific facts or opinions relating to an individual.

**What is personal and sensitive data?**

Personal information is information that identifies you as an individual and relates to you. This includes:

- Name;
- Address;
- Email address;

- Photographs;
- IP addresses;
- Location data;
- Profiling and analytics data; and
- Online Cookies.

Personal Sensitive Data is an additional category of data and consists of more in-depth data such as:

- Race;
- Trades Union Membership;
- Religion;
- Political Opinions;
- Sexual Orientation;
- Health Information;
- Biometric Information; and
- Genetic data.

**Anonymised and pseudonymised data**

As well as personal confidential data, Coast Academies uses the other categories of data which are designed to improve the safety of the individuals that it refers to, these categories are as defined below:

- **Anonymised data** – where unique identifiers such as your name and full address have been removed so the information is no longer personally identifiable; and
- **Pseudonymised data** – where personal information about you is replaced with a unique code. We retain the key to the code so would know which person this information relates to but a third party who we shared this data with would not. This is often used for example, when information is needed for research purposes.

Where possible, we will ensure that your information is anonymised or pseudonymised to protect the identities of the individuals.

Both the GDPR (2016) and the Data Protection Act (2018) also sets out specific rights for school pupils in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Pupil Information) (England) Regulations 2005.'

**Legal Framework**

The disclosure and use of confidential information must be both lawful and ethical. The right to confidentiality is protected by:

- Common law;
- Article 8 of the European Convention on Human Rights, now incorporated into UK law by the Human Rights Act (1998);
- Data Protection Act (2018); and
- General Data Protection Regulation (2016)

Whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for requiring that confidentiality obligations, as outlined in this document, must continue to apply.

**The General Data Protection Regulation Principles**

The GDPR sets out the principles of how personal data will be processed, this does not directly replace the principles set out in the Data Protection Act 1998, rather should be seen as an evolution and consolidation of the terminology. Under article 5 of GDPR, individual organisations must ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

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;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
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 is 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; and
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.

Further information of the principles can be located at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

**Breach of the GDPR Principles**

The ICO has the power to serve an enforcement notice upon an academy if there is a contravention of any of the Principles. Such a notice may be served on the individual school or an individual within the school. It is a legal requirement to respond to these notices and failure to do so, may result in prosecution.

Any individual who knowingly breaches the regulation or, if the breach is a result of negligence, will be held accountable and may be subject to legal and/or disciplinary proceedings.

**Human Rights Act 1998**

Article 8 of the Human Rights Act 1998 establishes a right to “respect for private and family life”. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their records. Current understanding is that compliance with the General Data Protection Regulation (2016) and the Common Law of Confidentiality should satisfy Human Rights requirements.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

**Common law duty of confidentiality**

The duty of confidentiality arises out of the common law duty of confidentiality, professional obligations, and also staff employment contracts (including those for contractors).

This legal duty is not embodied in an Act of Parliament but has been built up from case law where practice has been established by individual judgements.

The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.

**Breach of confidence**

A breach of confidentiality will arise when:

- A duty of confidentiality exists (i.e. there is a legitimate expectation that information will be held confidentially);
- The information has the necessary quality of confidence (the information need not be highly sensitive but it cannot be trivial, it will not be confidential if it is readily available by other means or has already been made public); and
- There is an unauthorised disclosure of the confidential information.

A breach of confidentiality may also breach the Human Rights Act 1998 and the General Data Protection Regulation (2016).

**Disclosing and using personal data**

There are occasions where the disclosure of personal or sensitive data is necessary, however this can only be achieved providing that the principles of the GDPR are met. Coast Academies is legally required to disclose data for the purposes of statistical analysis and general census requirements (https://www.gov.uk/topic/schools-colleges-childrens-services/data-collection-statistical-returns). Where possible, this data will be either pseudonymised or anonymised to protect the identity of individuals, or more commonly, data will be aggregated so that there is no issue with disclosure as no personal data will be disclosed.

Should there be a need to disclose any information, a data request form must be completed and passed to the Data Protection Officer for review and each case will be reviewed and a decision made based on the legal basis for processing, the Data Protection Officer reserves the right not to share information should the principles of GDPR not be met. A log of all disclosures will be maintained along with all disclosure decisions and method of transfer.

Legitimate grounds to share information can include:

- Informed consent to disclose the information;
- Legal obligation to disclose the information;
- Disclosure as part of a contracted activity (i.e. biometrics for canteen);
- Disclosure meets the criteria set out in GDPR and is for the benefit of Coast Academies;
- Prevention and detection of crime (Under the Data Protection Law Enforcement Directive).

The above list is not exhaustive. Any data transfers will be completed using the appropriate encrypted methods of transfer. No data will be transferred without appropriate protection.

Should you require any information regarding information sharing or requests, please contact the Data Protection Officer.

**Explicit consent as a basis for processing information**

Under GDPR consent is the paramount consideration and in all cases the information must be openly transparent. This specifically relates to explicit consent in which individuals are required to give positive opt in or out and cannot be generic. Consent is especially important when processing any sensitive data, as defined by GDPR. Processing of this information generally cannot take place without consent.

Coast Academies will take necessary steps to ensure that consent is not made under duress and ensure that the individuals are given all the necessary information to allow them to make an informed decision on consent. Coast Academies will ensure that any forms used to gather data on an individual will include a link to the Privacy Notice which explains the use and legal basis for holding the data.

All individuals have the right to dissent from sharing information. In cases such as this, Coast Academies will record the decision and steps will be taken to ensure that no further processing of data takes place.

**Subject Access Requests (SARs)**

Coast Academies operates in an open and transparent way and we will comply with the law in respect of individual rights. Coast Academies recognises that individuals' rights are particularly important in relation to the handling of confidential personal information.

The General Data Protection Regulation provides living individuals the right to access personal information and any supplementary information that relates to this under the "Subject Access Request" (SAR). This information will only be disclosed pursuant to a subject access request where an individual has been identified as the "Data Subject" or consent has been obtained to disclose information to a third party.

Any request for information should be completed on the Subject Access Request form (appendix 1) this should then be sent to the Data Protection Officer. If a third party is making the request they should ensure that the appropriate details are recorded. In all cases, 2 forms of appropriate identification must be provided, for example

- Passport;
- Driving licence;
- Birth certificate;
- Recent utility bill;
- Official letter (e.g. solicitors letter); or
- Bus pass.

In all cases, the requester should make any request in writing and no information should be given out over the telephone relating to a subject access request, with the exception of potential timeframes. Information must never be given to third parties without adequate evidence to prove authorisation.

Any member of staff receiving a subject access request should forward this directly to the Data Protection Officer for processing.

There is no longer a charge for this service and all requests must be processed within a month of initial receipt, however if the request is large or complex an extension of up to three months may be applied on top of the initial month, should this occur, the requester will be notified as soon as possible.

It should be noted that subject access only applies to living individuals, if it is the case that an individual is deceased, the Common Law Duty of Confidentiality applies.

**Disclosures required by law**

There may be occasions in which the school is required to share information with the necessary organisation such as law enforcement or local government, examples include:

- Health and Safety at Work Act 1974, Regulations on the Reporting of Injuries, Diseases and Dangerous Occurrences (1985 Sl No 2023 and 1989 No 1457);
- Section 29(3) of the Data Protection Act (2018) or Data Protection Law Enforcement Directive;
- Section 35 of the Data Protection Act (2018) in which the disclosure is required by the order of the courts.

With reference to section 29(3) requests, the Data Protection Officer should be involved from the start of the process and will make a judgement on the disclosure of the data based on risk factors and whether the non-disclosure will significantly damage the case. All requests will be submitted on the appropriate section 29(3) form (appendix 2).

Section 29(3) requests are not suitable in civil cases.

In other cases, it may be necessary to share information for the purposes of dealing with any current or prospective legal proceedings, in these cases, an appropriate request must be made to the Data

Protection Officer who will assess each case on its specific details. In cases such as this, it would be most appropriate for the requester to obtain a court order as this would ensure that the school was legally obligated to release the information.

**Disclosures relating to Safeguarding**

It may also be necessary to disclose information for the following purposes:

- To protect the vital interests of the individual, for example, the release of medical information should failure to release result in harm to an individual;
- To prevent serious harm to a third party that would occur if the information was not disclosed

In all cases a record of the disclosure will be maintained by the Data Protection Officer and the relevant Safeguarding Lead. It should be noted that in the case of a Safeguarding issue, the safety of the individual is paramount and a disclosure may be made without the approval of the Data Protection Officer, should this occur, a record of disclosure would still be created by the Data Protection Officer retrospectively. It should be noted that this would be in extreme cases only.

**Disclosures to third parties**

It may be necessary to procure the services of a third party to undertake services within the Academy. Many of these contractors will have access to personal information. In these cases, the contractors should familiarise themselves with this policy and ensure that they are familiar with the concepts of good information governance and ensure that they are in compliance with the GDPR principles. The following key requirements must be specified with include:

- Data Controller/Data Processor relationship – the school maintains control of any information which was specifically collected by the school for the purposes of education;
- An appropriate confidentiality clause;
- Compliance with the GDPR (2016);
- Integrity of the systems that the contractors have in place including RBAC, security of systems, breach reporting processes and assurance that data will be kept secure;
- Notification of any breaches of data, including notification to the ICO where appropriate;
- Roles within the organisation such as who controls subject access requests;
- Notification of changes to data providers or if there are plans to subcontract any services;
- An indemnity agreement.

Coast Academies will, as data controller, take reasonable steps to ensure that all contractors comply with the requirements set out in GDPR.

It is the responsibility of Coast Academies, as data controller, to take reasonable steps to ensure that contractors comply with all Data Protection Principles, and that any alleged breaches are investigated.

**Partnerships and information sharing**

Some external parties, working in partnership with the school, may request access to information or systems. No information will be shared with any third party until:

- Coast Academies has established the appropriate legal basis for sharing that information;
- Individuals have been informed and informed consent obtained (consent cannot be implied); and
- A specific information sharing agreement has been drafted which specifically sets out how the information can be used.

Any contractors with access to school systems should be given the minimum access to the system which is appropriately controlled including access to email, addresses, intranet and network drives.

**Access to other information**

The Freedom of Information Act 2000 (FOIA) gives individuals the right to access non-personal information held by the school. The organisation has specific guidance which highlights individual rights of access - please see the Freedom of Information policy.

**Publication of Information**

The school publishes several documents that include some personal data for example:

- Event information;
- Staff information on school websites

All staff have the right to opt out of having any data presented on the website or any other documents. If an individual dissents, this will be recorded, and the details restricted. Individual staff files are kept confidential between the individual, their line manager, the Head of School/Headteacher and Human Resources.

**Disclosures of Closed Circuit Television data (CCTV)**

There are CCTV systems operating within the premises for the purpose of protecting staff, pupils, and property. These CCTV systems are restricted to public areas in the schools such as corridors and communal spaces. Any data obtained in these systems will only be processed in a manner which is in compliance with Coast Academies' Privacy Notice and Data Protection registration.

In the case of public CCTV systems, in order to be classed as personal information (i.e. relates directly to the individual and affecting their privacy), the following points apply:

- The individual has to be the focus of the information; and
- The information indicates something significant about the person.

If a static camera is used for general security purposes, it does not focus on individuals, the zoom facility is not used/ it does not have a zoom facility, then it is not covered by the DPA, however a camera that can be remotely operated, can zoom in (it has pan and zoom facility), or track an individual, is covered by the DPA.

The school ensures that signs are in place to inform people when a CCTV system is in operation, and its purpose.

Anyone applying for school CCTV images under a Subject Access Request should complete the standard Subject Access form. If the Police request the data, a Section 29 (3) form (see appendix 2) must be completed.

Further guidance on CCTV, can be obtained from the ICO website (https://ico.org.uk/for-the-public/)

**Marketing**

Personal information may be required for the purposes of marketing (secondary purposes). In cases such as these, consent will be obtained from the staff and parents/carers.

The Telecommunications Regulations require that individuals must consent to their information being used for direct marketing purposes by telephone, or email. More information is available on the Direct Marketing Association Website at www.the-dma.org.

Individuals have the right under the GDPR to prevent their personal information from being processed for direct marketing purposes.

**Photographs and internet publishing**

Photographs of individuals are classed as personal data under the GDPR. Coast Academies may wish to use these photos from time to time on the school websites or on literature. In all cases, consent will be obtained from the parents or carers of the pupils or the staff members involved. A record of consent must be maintained for the use and should the individuals withdraw their consent, then the images must immediately be removed from the website or literature. Photographs of individuals who have left the school should not be used and will be destroyed at the end of their retention period unless there is specific consent. If photographs are received from an agency, it is Coast Academies' responsibility to ensure the agency has gained consent and written confirmation of this must be obtained.

Further information and guidelines on using photographs on the internet for schools can be found on the ICO website (www.ico.org.uk)

**Records Management**

Personal Information will be stored securely until it reaches the end of its retention period. Once records reach this period, they are subject to a confidential waste disposal process. Further details relating to this can be found in the Records Management policy. Any third parties processing information on our behalf will be required to provide evidence of destruction or return the data to the school for secure disposal.

A record will be kept of the information that has been destroyed (including date of destruction, description of the information, and reason for destruction). Further information can be found in the Records Management policy**.**

**Contacts**

John Harle – Data Protection Officer

Email: dataprotection@coastacademies.org.uk

**Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

*Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.*

**Linked policies**

Coast Academies Information Security policy

Coast Academies Records Management policy

Coast Academies Information Risk Management policy

**Appendices**

Appendix 1 – Subject Access Request Form

Appendix 2 – Section 29(3) Data Request form (Law enforcement)

Appendix 3 – Glossary of terms

**Appendix 1 – Subject Access Request form**

**Subject Access Request under the General Data Protection Regulation**

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

If you are applying for your own records, please complete sections 1, 4, 5 and 6.

If you applying on behalf of another individual, please complete all sections – ensure that the individual has signed section 3 in order for you to act on their behalf.

Here is the necessary information:

**1 – Data Subject –** Please complete this section for the person whose information is being requested

| | |
|---|---|
| Surname: | |
| Previous surname: | |
| First name(s) | |
| Contact telephone no: | |
| Date of birth: | |
| Postcode: | |
| Address: | |
| Email address: | |
| Relationship with the school | Please select:<br>Pupil / parent / employee / governor / volunteer<br>other (please specify): |

**2 – Details of Applicant –** Please complete this section if you are not the individual named in section 1 but you are authorised to act on their behalf according to section 3 below

| | |
|---|---|
| Surname: | |
| Previous surname: | |
| First name(s) | |
| Contact telephone no: | |
| Date of birth: | |
| Postcode: | |
| Address: | |

**3 – Third party disclosure –** Please complete this section to authorise the person identified in section 2 to act on your behalf

I hereby authorise Coast Academies to release personal data detailed in section 4 below to the person detailed in section 2 above.

| Name (Block Capitals) | Signed: |
|---|---|
| | |

**4 – Access Request**

Type of request – Please tick the relevant box below, tick view records/read only if you wish to view records. If you require a full copy of your health records, please tick full records

| **View/ read only** | **Please tick** |
|---|---|
| Your contact details | |
| Your child's medical record | |
| Your child's behaviour record | |
| Your child's attendance | |
| Other (*Please be as precise as possible)* | |
| **Full copy** | **Please tick** |
| Your contact details | |
| Your child's medical record | |
| Your child's behaviour record | |
| Your child's attendance | |
| Other (*please be as precise as possible)* | |

Under both the Data Protection Act 1998 and GDPR 2016, you do not have to give a reason for applying for access to data, however to save us time and resources, if you wish, it would be helpful to provide details below, informing us or the periods you require, along with details which you may feel have relevance. We will supply you with this information within 20 working days of this form being submitted.

Please provide as much information as possible about the records you require and specify if you require anything specific which we may hold:

| |
|---|
| |

**5 – Identification –** The person named in Section 1 (and Section 2) must provide copies of two types of identification i.e. passport, driving licence, birth certificate and additional proof of address i.e. bank statement, utility bill (please do not provide originals).

**6 – Authorisation –** Please read notes overleaf. I have read this form and authorise a subject access request to be carried out. I understand that a fee may be required prior to release of any information. I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the personal data detailed above under the General Data Protection Regulation

| Applicants signature: | Date: |
|---|---|
| | |

Please forward all completed forms to **dataprotection@coastacademies.org.uk**

| **Office use only** | |
|---|---|
| Date of receipt | |
| Proof of identification seen Y/N | |
| Confirmation of address seen Y/N | |
| Specify identification seen (e.g. passport, driving licence etc) | |
| Specify address confirmation (e.g. Utility Bill) | |

**Appendix 2 – Section 29 (3) DPA Request or Data Protection Law Enforcement Request**

I am making enquiries which are concerned with (tick the appropriate option):

☐ **The prevention and detection of crime**

☐ **The apprehension or prosecution of offenders**

**Nature of enquiry:**

| |
|---|
| |

**The Information sought is needed for:**

| |
|---|
| |

**I confirm that the personal data requested is required for this purpose/those purposes, and failure to provide the information, in my view, would be likely to prejudice that/those purposes.**

**This enquiry is confidential and should not be communicated to the data subject**

| | |
|---|---|
| **Name of requestor** | |
| **Authority** | |
| **Address** | |
| **Signed** | |
| **Print name (and number)** | |
| **Date** | |

| **Office Use** | |
|---|---|
| **Date Received** | **Date Returned** |
| | |

**Appendix 3 – Glossary of terms**

| | |
|---|---|
| Personal Information/data | Data which identifies a living individual, either directly from that information or from additional information which is in the possession of, or is likely to come into the possession of the data controller. It includes both factual information and expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. |
| Sensitive Personal Information | Personal data consisting of information about racial or ethnic origin, political opinions, religious or other beliefs, trades union membership, physical or mental health condition, sexual life, criminal proceedings or convictions. |
| Data Subject | The person the information is about. |
| Data Controller | Person, company or organisation who determines the purpose and manner of the processing of the personal information (the school is the data controller). |
| Data Processor | These may be separate organisations that process information on behalf of data controllers (e.g. a third party company supplying confidential waste management services). Data processors also have obligations under the DPA and must ensure that the information they handle is processed in accordance with the legislation. A contract should always be put in place with any data processor to cover off DPA compliance. |
| Processing | Applies to all uses of data - collecting, storing, retrieving, reading, amending, and destroying. |
| Notification | The Information Commissioner maintains a public register of data controllers. Notification is the process of adding a data controller's details to the register. All data controllers processing personal information are required under the Data Protection Act 1998 to notify unless they are exempt. |
| The Information Commissioner (ICO) | The Information Commissioner is an independent official appointed by the Crown to oversee the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. |
| Third Party | When this term is used in relation to personal data it means any person other than the data subject, the data controller or any data processor or other person authorised to process data on behalf of the data controller or data processor. |
| Consent | Consent is one of the grounds on which personal information may be processed lawfully. The data subject's consent is any freely given, specific and informed indication by which the data subject signifies agreement to personal information relating to him/her being processed. |

| | |
|---|---|
| Explicit Consent | In the case of sensitive personal information if consent is being sought it must be 'explicit'. The consent of the data subject should be absolutely clear and should cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purposes of the processing and any special aspects of the processing which may affect the individual. |
| Educational Record | Any record of information which:<br>• is processed by or on behalf of the governing body, or teacher of the school<br>• relates to any person who is or has been a pupil at the school<br>• originated from or was supplied by, or on behalf of:<br>• an employee of the LA which maintains the school<br>• a teacher (other than information processed by a teacher solely for their own use)<br>• or other employee of the school (including an educational psychologist engaged by the governing body under a contract for services)<br>• the pupil (to whom the record relates) or<br>• the parent of the pupil<br><br>It does not include information about the physical or mental health or condition of the data subject. The Data Protection (Subject Access Modification) (Health) Order 2000 applies to this information. |
| Parent/Carer | Has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child. |