Furness & Millom Primary Catholic Cluster

'For I know the plans I have for you,' declares the Lord, 'plans to prosper you and not to harm you, plans to give you hope and a future.' (Jeremiah 29:11)

Data Protection Policy

Headteacher	Chair of Governors
Signed:	Signed:
Date:	Date:

This policy will be reviewed annually/**bi-annually**/tri-annually.
This policy will be reviewed in **Summer 2020**.

Furness & Millom Catholic Cluster consists of: St Pius X Catholic Primary School, St Columbas Catholic Primary School, Sacred Heart Catholic Primary School, Holy Family Catholic Primary School, St James' Catholic Primary School, Our Lady of the Rosary Catholic Primary School, St Mary's Catholic Primary School

GENERAL DATA PROTECTION REGULATION

CONTENTS

GENERAL DATA PROTECTION REGULATION

1.0 STATEMENT OF INTENT

1.1 The School(s) is /are committed to protecting the rights and privacy of individuals in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 We are required to keep and process certain information about its pupils, staff and other individuals for various purposes such as:

- To support pupil learning;
- To monitor and report on pupil progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To ensure we operate efficiently and effectively;
- To recruit and pay staff;
- To collect fees;
- To comply with legal obligations to funding bodies and the government;
- To enable financial modelling and planning;
- To develop a comprehensive picture of the workforce and how it is deployed.

1.3 We may be required to share personal information about our pupils or staff with other schools, organisations, the LA and social services.

1.4 This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage and audio and video systems.

2.0 LEGAL FRAMEWORK

2.1 This policy has due regard to legislation, including, but not limited to the following:

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- Protection of Freedoms Act 2012

2.2 This policy also has regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3.0 ASSOCIATED POLICIES

3.1 This policy should be read in conjunction with the following policies and procedures:

- CCTV
- Safeguarding Policy (including Child Protection)
- Code of Conduct for School Employees
- Freedom of Information
- IT Acceptable Use Guidance for School Based Staff
- The Use of Images (Photography and Videos)
- Records Management policy

4.0 DEFINITIONS

4.1 'Personal data' refers to any information that relates to an identifiable, living individual ('data subject'). This could including information such as names, addresses, telephone numbers, photographs, expressions of opinion about an individual, or an online identifier (for example an IP address or roll number).

4.2 ‘Special categories of personal data’ refers to information which is broadly the same as 'sensitive personal data' previously referred to in the Data Protection Act (DPA) 1998. This includes biometric data, ethnicity, religious beliefs, data concerning health matters and actual or alleged criminal activities.

4.3 'Processing' refers to any operation which is performed on personal data such as: collection, recording, organisation, storage, alteration, retrieval, use, disclosure, dissemination or otherwise making available, combination, restriction, erasure or destruction.

4.4 ‘Data Controller’ refers to any individual or organisation who controls personal data, in this instance UVHS.

4.5 ‘Data Subject’ refers to an individual who is the subject of the personal data, for example:

- Employees (current and former),
- Pupils (including former pupils),
- Recruitment applicants (successful and unsuccessful),
- Agency workers (current and former),
- Casual workers (current and former),
- Contract workers (current and former),
- Volunteers (including members and governors) and those on work placements,
- Claimants.

5.0 COMPLIANCE

5.1 Compliance with this policy is the responsibility of all the members of the school (s) who process personal data (including governors).

5.2 Any breach of this policy will result in disciplinary procedures being invoked. A serious or deliberate breach could lead to dismissal.

5.3 Personal information will only be shared where it is lawful to do so and the third party agrees to abide by this policy and complies with the principles of the GDPR.

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

6.0 DATA PROTECTION PRINCIPLES

6.1 In accordance with article 5 of the GDPR, personal data will be:

a) Processed lawfully, fairly and in a transparent manner.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
d) Accurate and, where necessary, kept up-to-date; ensuring that inaccurate personal data is erased or rectified without delay.
e) Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

6.2 We will only process personal data in accordance with individuals' rights and will comply with article 5 of the GDPR in the following ways:

a) By making 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 purpose of the processing; any disclosures to third parties that are envisaged; an indication of the period for which the data will be kept, and any other information which may be relevant.
b) By ensuring that the reason for which the personal data was originally collected is the only reason for which it is processed, unless the individual is informed of any additional processing before it takes place.
c) By not seeking 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 is given by individuals, it will be destroyed immediately.
d) By reviewing and updating personal data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate. Individuals must notify the school if a change in circumstances means that their data needs to be updated. It is the responsibility of the school to ensure that any notification regarding a change is acted on swiftly. The school may also contact individuals to verify certain items of data.
e) By undertaking not to retain personal data for longer than is necessary to ensure compliance with the legislation, any other statutory requirements and the Records Management policy. This means the school will undertake a regular review of the information held.
f) By disposing of any personal data in a way that protects the rights and privacy of the individual concerned.

g) By ensuring appropriate technical and organisational measures are in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

6.3 Personal data may be stored for longer periods and may be processed solely for archiving in the public interest, scientific or historical research, or statistical purposes.

7.0 ACCOUNTABILITY

7.1 The School is the registered Data Controller with the Information Commissioner's Office (ICO) and is responsible for controlling the use and processing the personal data it has collected.

7.2 We will implement technical and organisational measures to demonstrate that data is being processed in line with the principles set out in this policy. This will include:

- Providing comprehensive, clear and transparent privacy notices (Appendix 1 and 2).
- Using data protection impact assessments (DPIA), where appropriate (Appendix 3).
- Recording activities relating to higher risk processing, such as the processing of special categories of personal data.

7.3 The privacy notices (Appendix 1 and 2) explain how we will share personal data with third parties. This will only occur following consent from the Data Protection Officer (DPO). The sharing of personal data is generally limited to enabling the school to perform its statutory duties or in respect to a child's health, safety and welfare.

7.4 Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- Individuals who provide personal data to us are responsible for ensuring that the information is accurate and up-to-date.

8.0 DATA PROTECTION OFFICER (DPO)

- The DPO for the school will be the Cluster Business Manager. They will:
- Inform and advise UVHS personnel about their obligations under this policy (including recognising a subject access request, data security and off site use).
- Ensure everyone is aware of, and understands, what constitutes a data breach.
- Provide annual training on the contents of this policy and develop and encourage best practice in the school.
- Liaise with any external data controllers engaged with our school.

- Monitor internal compliance, including identifying processing activities and checking the recording of activities related to higher risk processing, advising and checking DPIAs (including need, methodology and any safeguards) and conducting internal audits.
- Take responsibility for continuity and recovery measures to ensure the security of personal data.
- Ensure obsolete personal data is properly erased and retain a Destruction Log. This will include the document description, classification, date of destruction, method and authorisation.
- Be the point of contact with the ICO and co-operate with any requests.
- Maintain an up-to-date knowledge of data protection law in relation to schools.

8.2 The DPO will report to the Headteacher and provide an annual report with recommendations to the Governing Body.

9.0 LAWFUL PROCESSING

9.1 Personal data can be lawfully processed under the following conditions:

a) Consent of the individual has been obtained.
b) Compliance with a legal obligation.
c) Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
d) Performance of a contract with the individual or to take steps to enter into a contract.
e) Protecting the vital interests of an individual or another person.

9.2 Special categories of personal data can be lawfully processed under the following conditions:

a) Explicit consent of the individual, unless reliance on consent is prohibited by EU or Member State law.
b) Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim (provided the processing relates only to members or former members or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
c) Processing relates to personal data manifestly made public by the individual.
d) Carrying out obligations under employment, social security or social protection law, or a collective agreement.
e) Protecting the vital interests of an individual or another person where the individual is physically or legally incapable of giving consent.
f) The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
g) Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
h) The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

i) Reasons of public interest in the area of public health.

j) Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9.3 We collect and use workforce information for general purposes under paragraphs 9.1c and 9.2g of this policy which complies with Articles 6 and 9 of the GDPR. Under any other circumstances the legal basis for processing data will be identified and documented prior to data being processed.

10.0 CONSENT

10.1 It is not always necessary to gain consent before processing personal data (see paragraphs 9.1 and 9.2) but when it is, consent must be a positive indication.

10.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes (it cannot be inferred from silence, inactivity or pre-ticked boxes). Consent obtained on the basis of misleading information will not be a valid basis for processing.

10.3 Any forms used to gather personal data will be provided with a privacy notice (Appendix 1 and 2) and will indicate whether or not the individual needs to give consent for the processing.

10.4 A record will be kept documenting how and when consent was given.

10.5 If an individual does not give their consent for the processing and there is no other lawful basis on which to process the data, then the school will ensure that the processing of that data does not take place.

10.6 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

10.7 Consent can be withdrawn by the individual at any time.

10.8 Parental consent will be sought prior to the processing of a child's data except where immediate safeguarding concerns prevent it.

11.0 THE RIGHT TO BE INFORMED

11.1 Privacy notices regarding the processing of personal data (obtained either directly or indirectly) will be concise, written in clear, accessible language and free of charge (Appendices 1 and 2).

11.2 The school will include the following information in its privacy notices following the ICO code of practice:

- The identity and contact details of the data controller and DPO.
- The intended purpose of, and the legal basis for, processing the data.
- The legitimate interests of the data controller or third party.
- Any recipient or categories of recipients to whom the personal data will be disclosed.
- Details of transfers to third countries and the safeguards in place.
- The retention period or criteria used to determine the retention period.
- The existence of the right to access, rectification, object, erasure and withdraw consent.
- The right to complain internally and to a supervisory authority.

11.3 Where data is obtained directly from an individual, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of

personal data, as well as any possible consequences of failing to provide the personal data, will be provided at the time of collection.

11.4 Where personal data about an individual has been obtained indirectly, information regarding the source of the data and whether it was publicly accessible will be provided. This information will be supplied:

a) Within one month of having obtained the data.

b) If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

c) If the data are used to communicate with the individual, at the latest, when the first communication takes place.

12.0 THE RIGHT TO ACCESS

12.1 Individuals have the right to obtain confirmation that their personal data is being processed fairly or to submit a subject access request (SAR) to gain access to their personal data. In order to ensure individuals receive the correct information SARs must be made in writing and submitted to the Headteacher (Appendix 4).

12.2 The Headteacher will verify the identity of the person making the request before any information is supplied.

12.3 All requests will be responded to within one month of receipt.

12.4 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

12.5 Where a fair processing request is made the information contained within the relevant privacy notice will be provided.

12.6 Where a SAR is made copies of personal data will generally be encrypted and supplied to the individual in a commonly used electronic format.

12.7 Where a SAR is received from a pupil, the policy is that:

- It will be processed in the same way as any other SAR. The information will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Where a pupils does not appear to understand the nature of the request will be referred to their parents or carers.
- A SAR from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the information will be sent either in a sealed envelope or electronically to the requesting parent. This will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

12.8 In the event that a large quantity of information is being processed the individual may be requested to specify the information the request is in relation to.

12.9 Where a request is excessive or repetitive, a 'reasonable fee' will be charged. All fees will be based on the administrative cost of providing the information.

12.10 Where a request is manifestly unfounded the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reason behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

13.0 THE RIGHT TO RECTIFICATION

13.1 Personal data held by theschool will be as accurate as is reasonably possible.

13.2 Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where an individual informs the school of inaccurate or incomplete personal data their data record will be updated as soon as is practicable.

13.3 A printout of a child's personal data record held on the school's information management system will be provided to parents every twelve months so they can check its accuracy and make any amendments.

13.4 Where the personal data has been disclosed to a third party, the school will inform them of any rectification where possible. The individual will also be informed about the third parties that the data has been disclosed to where appropriate.

13.5 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

13.6 Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14.0 THE RIGHT TO ERASURE

14.1 Individuals have the right to request erasure of personal data. This applies where:

a) Personal data is no longer necessary for the purpose for which it was collected/processed.
b) Withdrawal of consent and no other legal ground applies.
c) The individual objects to the processing and there is no overriding legitimate interest.
d) Personal data is unlawfully processed.
e) Personal data has to be erased in order to comply with a law.
f) Personal data of a child is processed in relation to an online service.

14.2 The school has the right to refuse a request for erasure where personal data is being processed for:

a) Exercising the right of freedom of expression and information.
b) Compliance with legal obligations or for performing tasks carried out in the public interest or in exercising the data controller’s official authority.
c) Reasons of public interest in the area of public health.
d) Archiving purposes in the public interest, scientific or historical research, or statistical purposes.
e) The establishment, exercise or defence of legal claims.

14.3 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data.

14.4 Where personal data has been disclosed to third parties they will be informed about the request for erasure, unless it is impossible or involves a disproportionate effort to do so.

14.5 Where personal data has been made public and then is requested to be erased, taking into account the available technology and the cost of implementation, all reasonable steps will be taken to inform other data controllers about the request for erasure.

15.0 THE RIGHT TO RESTRICT PROCESSING

15.1 Individuals have the right to restrict the school's processing of personal data.

15.2 In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

15.3 The school will restrict the processing of personal data in the following circumstances:

a) Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data.

b) Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual.

c) Where processing is unlawful and the individual opposes erasure and requests restriction instead.

d) Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

15.4 If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

15.5 The school will inform individuals when a restriction on processing has been lifted.

16.0 THE RIGHT TO DATA PORTABILITY

16.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

16.2 Personal data can be moved, copied or transferred from one IT system to another in a safe and secure manner, without hindrance to usability.

16.3 The right to data portability only applies in the following cases:

a) Where personal data has been provided by an individual to the school

b) Where the processing is based on the individual's consent or for the performance of a contract.

c) When processing is carried out by automated means.

16.4 The school will respond to any requests for portability within one month and will provide the personal data free of charge and in a structured and commonly used form.

16.5 Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

16.6 In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

16.7 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of receipt of the request.

16.8 Where no action is being taken in response to a request the school will, without delay and at the latest within one month, explain the reason for this. The individual will also be informed of their right to complain to the supervisory authority and to a judicial remedy.

17.0 THE RIGHT TO OBJECT

17.1 The school will inform individuals of their right to object at the first point of communication. This will be outlined in a privacy notice (Appendix 1).

17.2 Individuals have the right to object to the following:

17.3 Processing based on legitimate interests or the performance of a task in the public interest.

17.4 Direct marketing.

17.5 Processing for purposes of scientific or historical research and statistics.

17.6 Where personal data is processed for the performance of a legal task or legitimate interests:

17.7 An individual's grounds for objecting must relate to his or her particular situation.

17.8 We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

17.9 Where personal data is processed for research purposes:

17.10 The individual must have grounds relating to their particular situation in order to exercise their right to object.

17.11 Where the processing of personal data is necessary for the performance of a public interest task, UVHS is not required to comply with an objection to the processing of the data.

18.0 PRIVACY BY DESIGN

18.1 We will act in accordance with the GDPR by adopting a 'privacy by design' approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

18.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with data protection obligations and meeting individuals' expectations of privacy (Appendix 3).

18.3 DPIAs will allow us to identify and resolve problems at an early stage, thus preventing reputational damage which might otherwise occur.

18.4 All DPIAs will include the following information:

- A description of the processing operations and the purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An outline of the risks to individuals.
- The measures implemented in order to address risk.

18.5 A DPIA will be used for new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

18.6 A DPIA will be used for more than one project, where necessary.

18.7 High risk processing includes, but is not limited to, the following:

18.8 Systematic and extensive processing activities.

18.9 Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

18.10 If a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

19.0 DATA BREACH NOTIFICATION

19.1 The term 'data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

19.2 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

19.3 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

19.4 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

19.5 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

19.6 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

19.7 Effective and robust breach detection, investigation and internal reporting procedures are in place, which will guide decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

19.8 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including categories, approximate number of individuals and records concerned.
- The name and contact details of the DPO.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

19.9 Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

20.0 DATA SECURITY

20.1 The school undertakes to ensure the security of the personal data it has collected. Personal data will only be accessible to those who have a valid reason for using it.

20.2 All the members of the school (including governors) are responsible for ensuring that any personal data they hold is kept secure and not disclosed to any unauthorised third party (a data security user checklist is provided for quick reference in Appendix 5).

20.3 **Physical measures**

- Premises security measures, such as alarms, safes, deadlocks, are in place.
- Only authorised persons are allowed in the IT office.
- Disks, tapes and printouts are locked away securely when not in use.

- Visitors to the school are required to sign in and out, wear identification badges and are, where appropriate, accompanied.
- Premises security and storage systems is reviewed on a regular basis. If an increased risk in vandalism/theft is identified, extra measures to secure data storage will be put in place.

20.4 **Technical measures**

a) Security software is installed on the school networks and electronic devices. This includes:
   - Internet filtering and firewall
   - Anti-virus
   - Email ransom ware detection

b) Data on the school network drives is password protected and automatically backed up offsite. There are procedures in place to access and restore all the data held on the school network drives should this be necessary.

c) All electronic devices are password protected and, where possible, have been enabled to allow remote blocking or deletion of personal data in the case of theft.

d) Authorised users are given a secure user name and password to access the school networks, One Drive, Google Suite, and any other learning platform they require access to.

e) Password rules have been implemented.

f) Authorised users will be assigned a clearance that will determine which files are accessible to them. Protected files are not accessible to unauthorised users.

g) Removable storage devices eg USB sticks, can only be used with the express permission of the Headteacher and under the following conditions:
   - The device **must** be supplied by the school (or encrypted by the IT technicians);
   - It **must** be password protected and encrypted;
   - It **must** be stored in a secure and safe place when not in use;
   - It **must not** be accessed by other users (e.g. family members).
   - Personal data **must** be securely deleted when no longer required.

h) Data breach detection tests will be undertaken to evaluate the school's technical measures and minimise the chance of a data breach.

20.5 **Organisational measures**

a) Follow the guidance set out in Appendix 7, Data Handling and Security Guidance..

b) Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.

c) Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation.

d) Paper records containing personal data **must** be kept secure if they are taken off the school premises.

e) Authorised users **must** sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically.

f) Passwords **must** be alphanumeric, including one capital and one special character, and be a minimum of 8 characters long to access the school network and One Drive, Google Suite, and other Office 365 services.
g) User names and passwords **must not** be shared.
h) Electronic devices (such as staff computers) **must** be locked even if left unattended for short periods.
i) Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.
j) Emails **must** be encrypted if they contain personal data and are being sent outside the school.
k) Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
l) Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
m) Visitors to the parts of school premises which contain special categories of personal data **must** be supervised at all times.
n) Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.
o) Personal data **must not** be disclosed to any unauthorised third parties.
p) School personal electronic devices **must not** be used to hold personal data.
q) Personal electronic devices **must** be password protected and have up-to-date, active antivirus and anti-malware checking software before being used to access personal data belonging to the school via:
   - A password protected removable storage device;
   - The remote desktop protocol (i.e. remote access to the school network);
   - One Drive and other Office 365 services.
r) Personal electronic devices that have been set to automatically log into the school network, school email accounts or One Drive that are lost or stolen must be reported to the DPO so that access to these systems can be reset.
s) If personal data is taken off the school premises, in electronic or paper format, extra care must be taken to follow the same procedures for security. The person taking the personal data off the school premises **must** accept full responsibility for data security.
t) Before sharing personal data, Staff/Governors **must** ensure:
   - They are allowed to share it;
   - That adequate security is in place to protect it;
   - Who will receive the personal data has been outlined in a privacy notice.
u) Any personal data archived on disks must be kept securely in a lockable cabinet.
v) School staff are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

21.0 CCTV AND PHOTOGRAPHY

21.1 The school understands that recording images of identifiable individuals constitutes as processing personal data and so is done in compliance with GDPR principles.

21.2 CCTV systems operate on the school premises for the purpose of protecting school members and property.

21.3 Pupils, staff, parents and visitors are notified of the purpose of collecting CCTV images via signage around the school premises.

21.4 Cameras are only placed where they do not intrude on an individual's privacy and are necessary to fulfil their purpose.

21.5 CCTV footage is kept for thirty days for security purposes unless it is relevant to an investigation in which case it will be kept for a maximum of six months. Detailed guidance is given in our CCTV policy.

21.6 We may occasionally use photographs/videos of pupils in a publication, such as the school website, prospectus, press release, or record a school play.

21.7 Prior to the publication of any photograph or video of pupils in the press, social media, school website and prospectus or in any other marketing or promotional materials, written consent will be sought from parents. Detailed guidance is given in the Photography and Videos at School policy.

21.8 Photographs or videos captured by other individuals for recreational or personal purposes, such as pupils taking photos on a school trip or parents taking photos at prize giving, are exempt from the GDPR.

22.0 DBS DATA

22.1 DBS information is treated as a special category of personal data under this policy.

22.2 DBS information will never be duplicated and any third parties who have lawful access to DBS information will be made aware of their GDPR responsibilities.

23.0 THE SECURE TRANSFER OF DATA

23.1 We are required to share personal information with the Department for Education (DfE), Education and Skills Funding Agency (ESFA), Cumbria County Council (CCC), Ofsted, schools and educational institutions, public services and other third party providers. These are outlined in the privacy notices (Appendix 1 and 2).

23.2 School staff and governors must not remove, copy or share any personal data with a third party without permission from the Head teacher and DPO.

23.3 Where personal data is required to be lawfully shared with a third party it must be securely transferred either through a portal or be sent following encryption, using approved encryption software, and be password protected.

23.4 No personal data will be transferred to a country outside the European Economic Area (EEA) without the explicit consent from the individual. Advice must be taken from the DPO.

24.0 PUBLICATION OF INFORMATION

24.1 A publication scheme can be found in the Freedom of Information policy and on the school website. This specifies the classes of information that will be made available on request, including:

24.2

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

24.3 We will not publish any personal data on the school websites without consent from the affected individual(s).

24.4 When uploading information onto the school websites consideration is given to any metadata or deletions which could be accessed in the documents and images.

25.0 DATA RETENTION

25.1 Personal data will not be kept for longer than is necessary.

25.2 The DPO will ensure that obsolete personal data is properly erased. The length of time we hold personal data is set out in our Records Management policy.

25.3 Personal data that is not required will be deleted as soon as practicable.

25.4 Some educational records relating to former pupils or employees may be kept for an extended period for legal reasons, the provision of references or for historical archives.

26.0 DATA DISPOSAL

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

26.2 Paper documents containing personal data 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.

26.3 Hard drives of redundant PCs and storage devices containing personal data will be securely wiped clean before disposal, or if that is not possible, physically destroyed.

26.4 The Headteacher will retain a Destruction Log of personal data that is disposed of. This will include the document description, classification, date of destruction, method and authorisation. This will be reviewed by the DPO periodically.

27.0 TRAINING AND AWARENESS

27.1 All school staff and governors will receive GDPR training on an annual basis led by the DPO. They are 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.

28.0 ENQUIRIES

28.1 Any further information, questions or concerns about this policy or the security of data held should be directed to the DPO, Mrs V Warner via email: vwarner@catholicschools.org.uk

28.2 General information about the GDPR can be obtained from the Information Commissioner's Office http://www.ico.gov.uk/.

28.3 This policy will be reviewed tri-annually and may be supplemented by additional procedures.

Appendix 1 - Privacy Notice: How we use Pupil Information

The categories of pupil information that we collect, process, 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);
- Contact information and contact preferences,
- Attendance information (such as sessions attended, number of absences and absence reasons).
- Assessment information (such as reports, feedback, test data and exam results)
- Relevant medical information (such as medication details, allergies, medical conditions and notes from meetings/GPs/other health care professionals)
- Special Educational Needs information (such as Education and Health Care Plans (EHCPs), Individual Education Plans (IEPs) and notes from review meetings and professional assessments)
- Safeguarding Information
- Exclusion and behaviour information
- Post 11 learning information and destination data
- CCTV images

Why we collect and use this information

We use the pupil data:

- To support pupil learning;
- To monitor and report on pupil progress;
- To provide appropriate pastoral care;
- To protect pupil welfare
- To assess the quality of our services;
- To comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information for general purposes under paragraphs 9.1c and 9.2g of the General Data Protection Regulations policy which complies with Articles 6 and 9 of the GDPR.

Less commonly we may process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent, the consent may be withdrawn at any time.

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. We may also receive information about pupils from other organisations such as their previous school, local authority and/or Department for Education (DfE).

Storing pupil data

The length of time we hold pupil information is set out in our Records Management policy.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us;
- Cumbria County Council;
- The Department for Education (DfE);
- The pupil's family and representitives

- Our regulator, Ofsted
- Supplies and service providers – to enable them to provide the service we have contracted them for
- Auditors
- Health and Social Welfare organisations
- Professional educational advisors
- Police , Courts and tribunals
- other public services that have a lawful right to collect pupil information;

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 pupil information with the DfE on a statutory basis. This information sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with the DfE under regulation 5 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 DfE (for example; via the school census) go to:

https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. 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 NPD go to:

https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

The DfE 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 DfE 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 the DfE releases data to third parties are subject to an 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 DfE's data sharing process go to:

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

For information about which organisations the DfE has provided pupil information (and for which project) go to:

https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE go to:

https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to their personal information. To make a request for your personal information, or be given access to your child's educational record, contact the Head teacher.

You also have the right to:

- object to processing of personal information 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;
- 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 information, we request that you raise your concern with us in the first instance. Alternatively, you can contact 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:

Mrs V Warner

Data Protection Officer

vwarner@catholicschools.org.uk

Appendix 2 - Privacy Notice: How we use School Workforce Information

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

- Personal information (such as name, employee or teacher number, national insurance number);
- Special categories of data including characteristics information (such as gender, age, ethnic group);
- Contract information (such as start dates, hours worked, post, roles and salary information);
- Work absence information (such as number of absences and reasons);
- Qualifications and, where relevant, subjects taught;
- Relevant medical or disability information (such as access arrangements, medication and occupational health reports);
- Payroll information (such as address, age, gender, bank account details);
- Pension details.

Why we collect and use this information

We use workforce data to:

- Ensure we can operate efficiently and effectively;
- Enable individuals to be paid;
- Allow for better financial modelling and planning;
- Enable the development of a comprehensive picture of the workforce and how it is deployed;
- Inform the development of recruitment and retention policies.

The lawful basis on which we process this information

We collect and use workforce information for general purposes under paragraphs 9.1c and 9.2g of the General Data Protection Regulations policy which complies with Articles 6 and 9 of the GDPR.

Collecting this information

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

Storing workforce information

The length of time we hold workforce information is set out in our Records Management policy.

Who we share this information with

We routinely share this information with:

- Cumbria County Council
- the Department for Education (DfE)
- other schools or organisations following reference requests
- other public services that have a lawful right to collect workforce information
- Payroll provider
- Next of Kin in emergency
- Our regulator, Ofsted
- Supplies and service providers – to enable them to provide the service we have contracted them for eg OHS
- Auditors
- Professional educational advisors
- Police , Courts and tribunals
- other public services that have a lawful right to collect pupil information;

Why we share workforce information

We do not share workforce information with anyone without consent unless the law and our policies allow us to do so.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment. We are required to share information about our workforce with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools. All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements including the data that we share with the DfE go to: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal 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 securely store and handle the data.

To be granted access to workforce information, organisations must comply with the DfE's terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of 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

To contact the DfE go to:

https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to your information. To make a request for your personal information, contact your Headteacher.

- 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;
- 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 collect or use your personal data, we ask that you raise your concern with your Headteacher . Alternatively, you can contact the Information Commissioner's Office at:

https://ico.org.uk/concerns/

Further information

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

Mrs V Warner: vwarner@catholicschools.org.uk

Data Protection Officer

Appendix 3 - Data Protection Impact Assessment (DPIA)

Section A – PIA screening questions

Question	Yes	No	Unsure	Comments
Will the project involve collecting new information about individuals?				
Will the project require individuals to provide information about themselves?				
Will information about individuals be disclosed to other individuals or organisations who have not previously held information about the individual?				
Is any information about individuals held for purposes it is not currently used for, or in a way it is not currently used?				
Will the project involve using a new technology that might be perceived as being intrusive to an individual's privacy?				
Will the project result in any decisions or actions taken against individuals which may have a significant impact on them?				
Will any information about individuals raise privacy concerns, e.g. information they may wish to keep private, such as criminal information held on DBS certificates?				
Will the project require you to contact individuals in ways that they may find intrusive?				

Section B – Identify the need

Section C – Provide the information flow

Section D – Practical steps

Section E – Risks to individuals and the school

Question	Yes	No	Unsure	Comments
Will there be adequate disclosure controls in place to decrease the likelihood of information being shared inappropriately?				
Will the context in which the information is used change over time, leading it to be used for a purpose that the individual may not be aware of?				
Will the project involve the introduction of any new surveillance methods?				
Could the measures used to gain information from the individual be perceived as intrusive in any way?				
Will data be shared between the school and other organisations? Is the individual aware of which information may be accessed?				
Will the project involve gaining information from individuals which may prevent them from remaining unidentified?				
Are individuals aware of the risks of identification and disclosure of information?				
Will gaining information mean that the school is no longer using information which is safely anonymised?				
Are appropriate procedures in place to ensure that information is not collected and stored unnecessarily, including ensuring that duplicate records are not created?				
Has an appropriate retention period been established?				

Risks to compliance

	Question	Yes	No	Unsure	Comments
Principle 1	Have you identified the purpose of the project?				
	Is there a lawful reason you can carry out this project?				
	Have you identified the social need and aims of the project?				
	Are your actions a proportionate response to the social need?				
	Have you established a process for how you tell individuals about how their personal data is used and stored?				
	Do you need to amend your privacy notices?				
	Have you established which conditions for processing data apply to the project?				
	If sensitive personal data is involved, have you established which conditions for processing this data apply?				
	If there is consent involved to use the personal data, is there an appropriate method in place for how this will be collected and what will be done if the data is withheld or withdrawn?				
	Will your actions interfere with the right to privacy, as outlined within the Human Rights Act 1998? If so, are the actions necessary and proportionate?				
Principle 2	Does the project plan cover all of the purposes for processing personal data?				
	Is there any personal data that could not be used, without compromising the needs of the project?				
Principle 3	Is the quality of the information sufficient enough for the purposes it will be used?				

	Is there any personal data that could not be used, without compromising the needs of the project?				
Principle 4	**If the procurement of new software is involved for the project, will it allow you to amend and delete information when necessary?**				
	Have you ensured that personal data obtained from individuals and/or other organisations is accurate?				
Principle 5	**Have you established a suitable retention period for the personal data you will be processing? (outline how long you will keep the data for)**				
	If you are procuring software, will this allow you to delete information in line with your retention periods?				
Principle 6	**Do you have a process in place to respond to subject access requests?**				

Principle 7	**Do any new systems provide protection against the security risks you have identified?**				
	If the project involves a new system, are measures in place to ensure staff receive appropriate training and instruction, so they understand how to operate the new system correctly?				
	Have relevant staff received appropriate training and instruction relating to data protection and information sharing?				
Principle 8	**Will the project require you to transfer data outside of the EEA? If yes, does the location ensure an appropriate level of protection?**				
	If data will be transferred outside of the EEA, are there appropriate measures in place to ensure that data is transferred securely?				

Section F – identify privacy issues and risks

Reference number	Privacy issue	Risk to individuals	Risk to compliance	Risk to school

Section G – Identify and approve the solutions

Reference number	Risk(s) identified	Risk score		Solution(s)	Result – is the risk accepted, reduced or eliminated?	Evaluation – is the risk to individuals acceptable after implementing the identified solutions?	Approved by (name and job role)
		Likelihood	Impact				

Section H – Integrate the PIA outcomes

Reference number	Action to be taken	Date for action to be completed	Anticipated risk score following action		Responsibility for action (name and job role)	Current status
			Likelihood	Impact		

Contact for future privacy concerns

Name	
Job role	
Email address	
Telephone number	

Appendix 4 - Access To Personal Data Request

(Subject Access Request – SAR)

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 ab out (i.e. the "Data Subject")?			YES / NO
If NO,			
Do you have the 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			
Description of Concerns/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 the GDPR 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 _____

Appendix 5 - Data Security User Checklist

- This checklist applies to all school staff and governors and refers to personal data belonging to this school (as the data controller):
- Paper records containing personal data must not be left unattended or in clear view anywhere with general access.
- Paper records and removable storage devices must be stored in a secure and safe place that avoids physical risk, loss or electronic degradation.
- Paper records containing personal data must be kept secure if they are taken off the school premises.
- All users must sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically.
- Passwords must be alphanumeric, including one capital and one special character, and be a minimum of 8 characters long to access the school network and devices. Passwords must be changed regularly.
- User names and passwords must not be shared.
- School electronic devices (such as staff computers) that are used to access personal data must be locked even if left unattended for short periods.
- Computer terminals, CCTV camera screens etc. that show personal data must be placed so that they are not visible except to authorised staff.
- Emails must be encrypted if they contain personal data and are being sent outside the school.
- Circular emails must be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
- Visitors must not be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
- Visitors to parts of the school premises containing special categories of personal data must be supervised at all times.
- Personal data must not be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.
- Personal data must not be disclosed to any unauthorised third parties.
- Removable storage devices (such as USB sticks) can only be used with the express **permission of the Headteacher** to hold personal data under the following conditions:
    - The device **must** be checked by an IT Technician before use;
    - It **must** be password protected and encrypted;
    - It **must** be stored in a secure and safe place when not in use;
    - It **must not** be accessed by other users (e.g. family members).
- Personal data must be securely deleted when no longer required.
- Personal electronic devices must not be used to hold personal data belonging to School.
- Personal electronic devices must be password protected and have up-to-date, active anti-virus and anti-malware checking software before being used to access personal data belonging to school.

- If personal data is taken off the premises, in electronic or paper format, extra care must be taken to follow the same procedures for security. The person taking the personal data off the school premises must accept full responsibility for data security.
- Before sharing personal data, staff and governors must ensure:
    - They are allowed to share it;
    - That adequate security is in place to protect it;
    - Who will receive the personal data has been outlined in a privacy notice.
- Any personal data archived on disks must be kept securely in a lockable cabinet.
- Staff **must i**nform their Headteacher if they want to process a new type of personal information
- Staff **must** inform the Headteacher if they want to share information with a new recipient / 3rd party
- Staff **must** inform the Headteacher if they want to register pupils on to a new App
- Staff **must** inform the Headteacher if they think there has been a breach
- Staff **must** always consider the protection of personal data when setting up or reviewing processes in school as a DPIA may be required.
- Electronic equipment eg PCs , laptops, etc must not be disposed of without the permission of the Headteacher who will arrange for the necessary processes to be carried out to ensure no data remains on the device.
- Staff are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

Appendix 6 - Third Party Suppliers Letter to confirm compliance with GDPR

Dear

Compliance with GDPR

As a third party supplier we need you to confirm that you have undertaken a review of your processes and procedures to comply with GDPR regulations. To continue with our commercial relationship we need confirmation of this and that the current contract reflects this. Please complete the series of questions below and explain how you will comply (the text is taken directly from the GDPR).

28(3) Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:

Requirement	Confirm consent and process
28(3)(a) process only on documented instructions, including regarding international transfers(unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);	
28(3)(b) ensure those processing personal data are under a confidentiality obligation (contractual or statutory);	
28(3)(c) take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;	
28(3)(d) only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;	
28(3)(e) assist the controller in responding to requests from individuals (data subjects) exercising their rights;	
28(3)(f) assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);	
28(3)(g) delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);	

28(3)(h) make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.	

APPENDIX 7
DATA CLASSIFICATIONS AND HANDLING REQUIREMENTS

This is an indicative rather than exhaustive guide to data classification and the resulting data handling requirements. All relevant queries should be directed to the Data Protection Officer .

	Public	Confidential	Sensitive
Impact if the information becomes public	**No risk**	**Low-Medium Risk** May result in minor reputational or financial damage to the school. May result in minor privacy breach for an individual.	**Medium-High Risk** Could substantially damage the reputation of the school, have a substantial financial effect on school or a third party, or would result in a serious privacy breach to one or more individuals.
Description of the information	Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain.	May result in minor reputational or financial damage to the school. May result in a minor privacy breach for an individual. Information that should only be available to sub-groups of staff within the school who need the information to carry out their roles.	Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.
Examples of information This list is indicative not exhaustive if unsure ask name/role for advice	● Prospectus ● Press releases ● Open content on the school web site ● Publicity flyers and leaflets ● Published information released under the Freedom of Information Act ● Policies, annual reports and financial statements ● Job adverts (excluding internal only positions) ● staff names and contact details ● Staff publications. ● Agendas and minutes of school committees and working groups (except reserved business). ● Patented intellectual property.	● Student personal details e.g. demographics, personal email address etc. ● Staff personal details e.g. demographic, payroll number, personal email address etc. ● Internal only school policies, processes and guidelines. ● Internal only job adverts. ● Tender bids prior to award of contract ● Individual's salaries ● Student's assessment marks. ● Job application responses/CVs (unless they contain sensitive personal information).	Sensitive personal data and some other data. ● Exam questions prior to use ● Medical records ● UPRNs ● Usernames and passwords ● Investigations/disciplinary proceedings. ● Payment card details. ● Financial information (banking details and data not already disclosed in financial statements). ● Passwords and access codes to school systems. ● Some complaints or requests ● Biometric data

	Public	Confidential	Sensitive
Security Marking	No marking required	Must be clearly marked as **Confidential**	Must be clearly marked as **Sensitive**
Storage (electronic)	● Store using school IT facilities to ensure appropriate management, back-up and access. ● Use only the school approved cloud service [insert name here]. Some cloud services may **not** be used because they link to computer C: drives which is not secure.	● Store only on the school IT network and never on the C: drive of a PC/laptop (beware downloading information when a laptop is not connected to the school domain - the download will go onto the C: drive and you may be in breach of this policy). ● Store only on the C: drive of a specially encrypted PC/laptop. ● Store only on the approved cloud service in a suitably restricted folder. ● Portable devices such as USB sticks must be encrypted and must **not** be used for long term storage due to the risks of loss or corruption of data. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any unencrypted school device e.g. tablet, laptop, mobile phone etc.	● Store only on the school IT network in rigorously monitored & restricted access drives. ● Never to be stored on the approved cloud service unless also separately encrypted. ● Never to be stored on any portable storage device i.e. USB drive regardless of encryption. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any school device e.g. tablet, laptop, mobile phone etc. unless it has been specially encrypted *and* there are other high level procedural safeguards.
School Website	No restrictions	Not permitted	Not permitted
Storage (hardcopy)	No restrictions	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.
Email hosted by school	No restrictions	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone. Emails to internal recipients i.e. school email account-to-school	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone. Emails to internal recipients i.e. school email account-to-school email account

	Public	Confidential	Sensitive
		email account are secure, so encryption and encrypted attachments are not necessary.	are secure, so encryption and encrypted attachments are not necessary.
Personal email account e.g. Hotmail etc.	No restrictions	Not permitted	Not permitted
Post (Internal)	No restrictions	In a sealed envelope marked Confidential.	Seal envelope, mark Confidential & hand deliver.
Post (External)	No restrictions	Tracked and recorded delivery only and marked Confidential	Tracked and recorded delivery only and marked Confidential within two separate envelopes.
School-based server	No restrictions but consideration should be given to back-up requirements.	No storage or creation is permitted unless the server environment is equivalent to the school-based server or the CTU server environment.	No storage or creation permitted unless the server environment is equivalent to the school-based server or the CTU server environment.
School owned laptop	No restrictions but do **not** use to store master copies of vital records.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.
Personally owned mobile device	No restrictions	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.	Not permitted unless authorised by the Senior Information Risk Owner (SIRO). Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.
School owned desktop (public areas)	No restrictions, but always lock the screen when unattended.	Not permitted. The risk of incidental disclosure is too high.	Not permitted. The risk of incidental disclosure is too high.
School owned desktop (key/card access controlled areas)	No restrictions, but always lock the screen when unattended.	Only permitted on encrypted drives or using or password protected files. Always lock the screen when unattended.	Only permitted on encrypted drives. Always lock the screen when unattended.
School owned mobile device	No restrictions, but always lock the screen when unattended.	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document.	Not permitted unless authorised by the SIRO. Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document

	Public	Confidential	Sensitive
Removable media (CDs, USB drives etc.)	No restrictions.	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase, digits and special characters.	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase, digits and special characters.
Disposal	No restrictions. Recycle where possible.	Shred or place in a confidential waste bag. Delete from electronic media when no longer required.	Cross shred only & put shredded material into the confidential waste. Appropriately scrub data from devices. Some devices (encrypted USB drives) may need to be securely destroyed. Seek advice from the IT manager.