Data Protection Policy

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Accountability
4. Data protection officer (DPO)
5. Lawful processing
6. Consent
7. The right to be informed
8. The right of access
9. The right to rectification
10. The right to erasure
11. The right to restrict processing
12. The right to data portability
13. The right to object
14. Automated decision making and profiling
15. Data protection by design and default
16. Data Protection Impact Assessments (DPIAs)
17. Data breaches
18. Data security
19. Safeguarding
20. Publication of information
21. CCTV and photography
22. Cloud computing
23. Data retention
24. DBS data
25. Monitoring and review

Statement of intent

Carmel College is required to keep and process certain information about its staff members, students, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The college may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, DfE, other colleges and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the college complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and the college believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Student Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE (2023) 'Keeping children safe in education 2023'

This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- ESFA Accountability Agreement

This policy operates in conjunction with the following college policies:

- IT and Social Media Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Freedom of Information Policy
- Records Management Policy

2. Applicable data

For the purpose of this policy, **'personal data'** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
  - Racial or ethnic origin.
  - Political opinions.

- Religious or philosophical beliefs.
- Trade union membership.
- Principles.

‘Sensitive personal data’ does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, colleges are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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 incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with” the above principles.

3. Accountability

The college will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

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

The college will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

The college will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)

Colleges are required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the college and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the college's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the college's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the college community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to colleges. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at the college, which is the governing body.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained

- Processing is necessary for a contract held with the individual, or because they have asked the college to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the college in the performance of its tasks

The college will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- 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
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
    - 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 with a basis in law
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.

- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

The college has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Students and their families
- College workforce
- Third parties
- Governors
- Volunteers

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where the college relies on:

- 'Performance of contract' to process a student's data, the college considers the student's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a student's data, the college takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a student's data, the college ensures that the requirements outlined in the 'Consent' section are met, and the college does not exploit any imbalance of power in the relationship between the college and the student.

6. Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The college ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to

ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When students and staff join the college, the staff member or student (or, where appropriate, student's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the college opts to provide an online service directly to a student, the student is aged 16 or over, and the consent meets the requirements outlined above, the college obtains consent directly from that student; otherwise, consent is obtained from whoever holds parental responsibility for the student, except where the processing is related to preventative or counselling services offered directly to student. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the college on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and students have the same right to be informed about how the college uses their data. The privacy notices supplied to individuals, including students, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time
    - Lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the college holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided – this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

8. The right of access (Appendix 2 and Appendix 3)

Individuals, including students, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing (Appendix 2 and Appendix 3) . The college will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the college may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a SAR has been made for information held about a student, the college will evaluate whether the student is capable of fully understanding their rights. If the college determines the student can understand their rights, it will respond directly to the student.

All requests will be responded to without delay and at the latest, within one month of receipt. 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.

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

The college will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the college will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

In the event that a large quantity of information is being processed about an individual, the college will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

9. The right to rectification

Individuals, including students, are entitled to have any inaccurate or incomplete personal data rectified.

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

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the college may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The college reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

The college will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The college will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, the college will inform them of the rectification where possible. Where appropriate, the college will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the college 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.

10. The right to erasure

Individuals, including students, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including students, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a student

The college will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

The college has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

The college has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the college may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a student 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 student has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the college will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The right to restrict processing

Individuals, including students, have the right to block or suppress the college's processing of personal data.

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

- Where an individual contests the accuracy of the personal data, processing will be restricted until the college has verified the accuracy of the data
- Where an individual has objected to the processing and the college is considering whether their legitimate grounds override those of the individual

- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the college no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, the college 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. The college will inform individuals when a restriction on processing has been lifted.

Where the college is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

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

The college reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12. The right to data portability

Individuals, including students, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The college will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

The college will provide the information free of charge.

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

The college will respond to any requests for portability within one month. 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 the receipt of the request.

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

13. The right to object

The college will inform individuals, including students, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals, including students, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

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

- An individual's grounds for objecting must relate to his or her particular situation.
- The college will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the college can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The college will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and the college will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The college cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The college will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the college is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the college will offer a method for individuals to object online.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The college will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, the college will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. Automated decision making and profiling

The college will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a student nor use special category personal data, unless:

- The college has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

The college will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

The college will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

The college will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the college will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15. Data protection by design and default

The college will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the college has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the college will ensure that only data that is necessary to achieve its specific purpose will be processed.

The college will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in college ICT systems.
- Implementing basic technical measures within the college network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

16. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the college's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the college to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the college's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

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

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The college will ensure that all DPIAs 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

Where a DPIA indicates high risk data processing, the college will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

17. Data breaches (Appendix 4)

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Principal will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

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

Where the college faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the college becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. 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. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and 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

Where notifying an individual about a breach to their personal data, the college will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

The college will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

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

The college will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

18. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. Where digital data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the college enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Where possible, staff and governors will not use their personal laptops or computers for college purposes. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

If staff and governors need to use their personal laptops for college purposes, particularly if they are working from home, they will bring their device into college before using it for work to ensure the appropriate software can be downloaded and information encrypted.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending.

Before sharing data, all staff will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the college premises accepts full responsibility for the security of the data.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the college containing sensitive information are supervised at all times.

The physical security of the college's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.

The college will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

The college takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The IT Services Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

The college holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

19. Safeguarding

The college understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping students safe.

The college will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect students. The governing body will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a student in a timely manner.

The college will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a student is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The college will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a student at risk. The college will manage all instances of data sharing for the purposes of keeping a student safe in line with the Safeguarding and Child Protection Policy.

Students' personal data will not be provided where the serious harm test is met. Where there is doubt, the college will seek independent legal advice.

20. Publication of information

The college publishes a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:

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

Classes of information specified in the Freedom of Information Publication Scheme are made available quickly and easily on request.

The college will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the college website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

The college understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The college notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for six months for security purposes; the Estates Manager is responsible for keeping the records secure and allowing access.

Before the college is able to obtain the data of students or staff, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

The college will always indicate its intentions for taking photographs of students and will retrieve permission before publishing them. If the college wishes to use images or video footage of students in a publication, such as the college website, prospectus, or recordings of college plays, written permission will be sought for the particular usage from the student. Precautions are taken when publishing photographs of students, in print, video or on the college website.

Images captured by individuals for recreational or personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

Parents and others attending college events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the college.

The college asks that parents and others do not post any images or videos which include any students other than their own on any social media, or otherwise publish those images or videos.

22. Cloud computing

For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the college accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the college.

All files and personal data will be encrypted before they leave a college device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on college devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the college should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the college's policies for the use of cloud computing.

The college's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the college's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the college decide to withdraw from the cloud service in the future.

- Assess the level of risk regarding network connectivity and make an informed decision as to whether the college is prepared to accept that risk.
- Monitor the use of the college's cloud service, with any suspicious or inappropriate behaviour of students, staff or parents being reported directly to the Principal

23. Data retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former students or employees of the college may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

24. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

25. Monitoring and review

This policy is reviewed annually by the DPO. The next scheduled review date for this policy is June 2025.

File Name/Path	O:\Policies\2023-24 Policies			
Intranet Path	CONNECT>>DEPARTMENTS>>COLLEGE POLICIES>			
Circulation List	Principalship	✓	College Union Representatives	✓
	Full Governing Body	✓	HR Department	✓
Author / Responsibility	Vice Principal (Finance, Resources & Systems)			
Reviewed by:	Audit Committee			
Approved by:	Full Governing Body			
Date of last Policy approval:	July 2024			
Review interval:	Every year			
Date next review due:	July 2025			

Appendix 1

College as Data Controller

The College as Data Controller

Carmel College is the data controller and the Governing Body is therefore ultimately responsible for its implementation.

The types of information held by the College and how they are used are detailed in the College's registration issued by the Information Commissioner (ICO) under the reference Z6391538. The registration papers are available via the Information Commissioner's Office (ICO) website (www.ico.org.uk) or from the designated Data Protection Officer.

The designated Data Protection Officer will deal with the implementation of agreed policy and day-to-day matters along with the nominated staff:

Designated Data Protection Officer	Vice Principal (Finance, Resources and Systems)
Deputy Designated Data Protection Officer	HR Manager

Key nominated data protection staff:

Staff records	College HR Manager
Student records	College MIS Manager
Student welfare records	Designated Safeguarding Lead
College examination records	College Examination Manager
College IT data/infrastructure	College IT Manager
College marketing materials	College Marketing, Liaison & Admissions Manager
College financial records	College Finance Manager
College health and safety records	College Estates Manager

Appendix 2

Subject Access Request Guidance

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Handling requests
4. Requests on behalf of a student
5. Seeking clarification
6. Charges
7. Finding and sending information
8. Exemptions and refusing requests
9. Record-keeping
10. Monitoring and review

Statement of intent

A subject access request (SAR) is a request made by, or on behalf of, an individual for the information which they are entitled to ask for under Article 15 of the UK GDPR. At Carmel College, we are committed to upholding the right of individuals to obtain a copy of their personal data, as well as other supplementary information, to provide transparency in how and why the college uses such data. This guidance sets out how the college will:

- Recognise and respond to SARs.
- Provide the information requested.
- Always consider student wellbeing.
- Refuse requests, where appropriate.

Routine verbal enquiries and correspondence that covers information that is provided routinely and can be managed quickly in the normal course of the college's business, e.g. a request by a staff member to see their employment contract, are not considered to be SARs and are not considered under this guidance.

1. Legal framework

This guidance has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Data Protection Act 2018
- DfE (2023) 'Data protection in schools'
- UK GDPR

This guidance operates in conjunction with the following college policies:

- Data Asset Register
- Data Protection Policy
- Freedom of Information Policy
- Records Management Guidance

2. Roles and responsibilities

The governing body will be responsible for:

- Ensuring the college respects the rights of individuals to obtain copies of their personal information.
- Ensuring the college obtains legal advice as required when handling SARs.

The principal will be responsible for:

- Ensuring all staff understand how to recognise a SAR.
- Ensuring relevant staff receive detailed training on handling SARs in line with their job responsibilities.

- Ensuring the wellbeing of students is always taken into account when handling SARs.

The DPO will be responsible for:

- Overseeing the management of all SARs received by the college.
- Ensuring all relevant staff understand their roles and responsibilities in relation to complying with SARs.
- Identifying which staff members should receive specific training on SARs.

The DSL will be responsible for:

- Advising the DPO as necessary on possible safeguarding concerns when handling SARs.

All staff will be responsible for:

- Identifying SARs and understanding the next steps.
- Making entries on the SAR Log as appropriate.
- Following instructions and advice from the DPO on how to handle SARs.

3. Handling requests

Anyone whose personal data is controlled by the college can submit a SAR, including students, parents, staff, volunteers and governors. Where a request is made for data for which the college is a processor but not a controller, it will inform the requester and refer them to the controller.

The college will treat any request where it is clear that an individual is asking for their own personal data, and which is outside of the college's normal course of business, as a SAR. The DPO will determine whether enquiries that are not formal requests for information should be processed as a SAR on a case-by-case basis.

The college may receive requests for personal data which refer to the Freedom of Information Act 2000 in error – these will still be processed as SARs. Legitimate freedom of information requests will be handled in line with the Freedom of Information Policy.

All office staff, and any other staff identified by the DPO, will receive specific training on how to identify a SAR and the next steps to take. All SARs will be forwarded to the DPO, upon receipt, for oversight. The college will treat all SARs the same regardless of how they are received, e.g. in writing, verbally or through social media.

The SAR will be acknowledged as soon as possible to the requester, with a timeframe set out for the response. Requests will be responded to within one calendar month from the date received, e.g. a request on 1 January will have a deadline of 1 February. Where there is no corresponding calendar date, the date for response is the last day of the following month, e.g. a request on 31 August will have a deadline of 30 September. Where the corresponding date falls on a weekend or public holiday, the deadline will be the next working day.

Identity verification

To avoid personal data being sent to someone who does not have a right to access it, the college will ensure it is satisfied that the identity of the requester or the person the request is made on behalf of is known. Requests for identity verification will be made promptly. The deadline for responding will begin only after the requester's identity has been verified. Alternatives to requesting formal identification will be considered, and formal identification will only be requested to verify a requester's identity where necessary, e.g. who they are is not obvious to the college, or there is the possibility of deception. The DPO will determine what information the college requires to verify an individual's identity and explain to them what they need to provide.

Requests by a student

Where a request is from a student, the college will consider the extent to which the student is mature enough to understand their rights. Typically, a student will be presumed to possess sufficient maturity, but the college will decide on a case-by-case basis. Where the college is confident the student understands their rights, it will respond directly to the student. If not, the student will be informed that they will need to ask their parent/guardian to make a request on their behalf.

Complex requests

Where a request is deemed to be complex, the response deadline will be extended by an extra two calendar months. The individual will be notified within one month of receiving their request of the decision, with a clear explanation of why it has been deemed complex.

In deciding whether a request is complex, the DPO will consider the college's circumstances and the specifics of the requests. Examples of where a request may be complex include, but are not limited to, the following:

- Technical difficulties in retrieving the information, e.g. it is electronically archived
- Applying an exemption that involves large volumes of particularly sensitive information
- Clarifying potential issues around disclosing information about a student to a legal guardian
- Any specialist work involved in obtaining the information or communicating it in an intelligible form
- Clarifying potential confidentiality issues around the disclosure of sensitive medical information to an authorised third party
- Specialist legal advice is required
- Searching large volumes of unstructured manual records

Requests involving a large volume of information will be considered a factor that can add to the complexity of a request, but a request will not be deemed complex solely on this basis.

Third party requests

The college will ensure the third party is entitled to act on behalf of the individual, e.g. by requesting a written authority signed by the individual confirming they give the third party permission to act on their behalf. Where there is insufficient evidence to satisfy the college that the third party is authorised to act on the individual's behalf, the SAR will not be complied with. A response will be provided to the requester to explain this.

Where the college believes an individual may not understand the nature of the information being disclosed and is concerned about disclosing excessive information, the college will contact the individual to make them aware and may agree to send the response directly to the individual rather than the third party.

Simultaneous requests

Where an individual makes a number of other requests relating to other rights, e.g. the right to erasure and the right to data portability, each request will be managed separately. The deadline for the SAR will be extended by two months; the individual will be notified with an explanation as soon as possible, and within one month at the latest.

4. Requests on behalf of a student

Where a parent makes a request to see what the data the college holds about their child, the college will first check if:

- The requester has parental responsibility.
- The student has given their consent for a parent or carer to act on their behalf.
- Releasing the information to an absent parent or carer would cause the student distress or result in safeguarding concerns.

The college will allow parents to exercise their child's rights on their behalf where authorisation is provided, or it is evident that this is in the student's best interests. The college will consider the following when a parent, or someone else authorised by the student, makes a SAR on the student's behalf:

- Any court orders relating to parental access or responsibility that may apply
- The duty of confidence owed to the student
- Any consequences of allowing those with parental responsibility, or those authorised to act on their behalf, access to the student's information
- Any detriment to the student if individuals with parental responsibility, or their authorised representatives, cannot access this information
- Any views the student has on whether others should have access to information about them

The DSL will be consulted if there is information of a sensitive nature that it may not be in the best interests of the student to be shared. The college will not provide a student's personal data, including their educational record, to a parent or carer if there is a court order in place that limits the exercise of their parental responsibility.

Where a student authorises someone other than a parent or carer to make a SAR on their behalf, the college will not respond if there are reasonable concerns that the student is acting against their own best interests, e.g. they are being pressured to make the SAR. Such concerns will be reported to the DSL immediately.

5. Seeking clarification

Where it is not fully clear what personal data the individual wants, the college will ask for clarification as soon as possible, with an explanation, to specify the information or processing activities the request relates to before responding. Clarification will not be required in usual circumstances, and will be limited to requests where it is genuinely required in order to respond and where the college processes a large amount of information about the individual.

The deadline for responding to the request will be paused until clarification is received, and the requester will be made aware of this. Once the requester responds, the deadline will resume with an extension by the number of days taken for a response. Where the college receives a request that is genuinely unclear whether an individual is making a SAR, the time limit to respond will apply from the date that clarification is received.

Where the requester responds repeating the original request or declines to provide any additional information, the SAR will be complied with by making reasonable searches for the information.

6. Charges

Requesters will not typically be charged for the college's compliance with a SAR. The college may, however, decide to charge a reasonable fee for administrative costs where:

- A request is manifestly unfounded or excessive.
- An individual requests further copies of their data following a request.

In determining a reasonable fee, the administrative costs will be considered for:

- Assessing whether the college processes the information.
- Locating, retrieving and extracting the information.
- Providing a copy of the information, e.g. photocopying, printing and postage costs.
- Communicating the response to the individual, including contacting the individual to inform them that the college holds the requested information.
- Staff time in performing all of the above.

The costs of staff time will be based on the estimated time it will take staff to comply with the specific request, charged at a reasonable hourly rate.

Requests for a fee will be sent as soon as possible, and within one calendar month of receiving the SAR. When requesting a fee, the costs will be explained to the individual, including a copy of the criteria used to determine it. The individual will be notified if the college intends to charge, even if the information is not being provided.

Where a charge is determined, the SAR will not be complied with until it is paid. Where no response is received within one month, the DPO will decide if it is appropriate to close the request on a case-by-case basis.

7. Finding and sending information

Finding information

The college will make reasonable efforts to find and retrieve the information requested. Searches will not be conducted that are unreasonable or disproportionate to the importance of providing access to the information. To determine this, the following will be considered:

- The circumstances of the request
- Any difficulties involved in finding the information, e.g. if technical expertise is required
- The fundamental nature of the right of access

If certain information is determined to be unreasonable or disproportionate, the college will still search for any other information within the scope of the SAR. The DPO will have regard to guidance from the ICO on finding and retrieving information to ensure adherence to UK GDPR for all SARs.

Routine management and changes as part of the college's processing activities will be allowed to proceed as normal for personal data in line with the Data Protection Guidance and Records Management Guidance; however, the DPO will ensure that all staff understand that data must not be amended or deleted with the intention of preventing its disclosure under a SAR.

Sending information

Individuals will receive the following information:

- Confirmation that the college is processing their personal data
- A copy of their personal data
- Other supplementary information

In addition to the above, the information below will be supplied:

- The college's purposes for processing
- Categories of personal data being processed
- Recipients or categories of recipient the college has or will be disclosing the personal data to
- The retention period for storing the personal data or, where this is not possible, the criteria for determining how long it will be stored
- The individual's right to request rectification, erasure or restriction or to object to processing
- The individual's right to lodge a complaint with the ICO
- Information about the source of the data, if the college did not obtain it directly from the individual

- Whether or not the college uses automated decision-making, including profiling, and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual
- The safeguards provided where personal data has or will be transferred to a third country or international organisation.

If the information above is provided in the college's privacy notice, a link to or a copy of the notice may be provided instead.

Prior to sending any personal data, information will be thoroughly checked to see if anything should be redacted, e.g. references to other individuals. The destination, e.g. email or postal address, will be checked to ensure it is correct. The DPO will ensure information is sent securely, with consideration given to the nature and sensitivity of the data.

Information provided will be explained, where necessary, to ensure it is easily understandable, e.g. clarifying the meaning of an attendance code.

Where a SAR is made verbally or through social media, the college will ask for an appropriate delivery address for the response. The college will respond to all SARs in a commonly used electronic format unless the requester asks for it to be provided in another commonly used format. Information will typically be provided via copies of relevant sections of original documents.

Where the response is requested to be verbal, the college will accept, provided the individual's identity is confirmed and only a small amount of information is requested. A record will be kept of the date, who provided the information, and what was shared.

Reasonable adjustments will be made to the format of the response, as required, to facilitate and comply with SARs made by an individual with a disability, in line with their specific needs.

Where the college has concerns, e.g. about security, over the method the individual has requested their information, the DPO will contact them as soon as possible to explain the college's concerns and ask for an alternative address or method.

8. Exemptions and refusing requests

SARs will be refused wholly or in part where:

- An exemption applies.
- It is manifestly unfounded or manifestly excessive.
- Complying would cause serious harm to the physical or mental health of any individual, provided the college has obtained an opinion within the last six months from an appropriate health professional that the serious harm test is met.

All SARs will be considered on a case-by-case basis and in the context in which it is made before a decision is made to refuse to it. Where an individual genuinely wants to exercise their right to access, the college will not refuse the SAR without strong justification.

Following a refusal, the college will inform the individual of:

- The reasons why.
- Their right to make a complaint to the ICO.
- Their ability to seek to enforce their right through the courts.

The college will be as transparent as possible on the reasons for withholding information; however, where telling an individual that a particular exemption applies would prejudice the purpose of that exemption, the response will be generalised.

A record of when and why a decision was made to refuse a SAR, in whole or in part, will be maintained on the SAR Log.

Manifestly unfounded requests

The college will refuse to comply with a SAR wholly or partly where it is determined to be manifestly unfounded. This will apply where an individual has no clear intention to exercise their right of access, e.g. they offer to withdraw the SAR in return for some form of benefit, or the request is malicious in intent and is being used to harass the college to cause disruption. Examples of malicious requests include, but are not limited to, where an individual:

- Explicitly states in the request or other communications their intent to cause disruption.
- Makes unsubstantiated accusations against the college or specific employees.
- Targets a particular employee against whom they have a personal grudge.
- Systematically sends different requests to the college, e.g. once a week, as part of a campaign.

Manifestly excessive requests

The college will refuse to comply with a SAR wholly or partly where it is determined to be manifestly excessive, i.e. it is clearly or obviously unreasonable. The DPO will consider whether the request is proportionate when balanced with the burden or costs involved in dealing with it, and consider the following circumstances:

- The nature of the requested information
- The context of the request, and the relationship between the college and the individual
- Whether a refusal to provide the information, or even acknowledge if the college holds it, may cause substantive damage to the individual
- The college's available resources
- Whether the request largely repeats previous requests and a reasonable interval has not elapsed
- Whether it overlaps with other requests

Information about other individuals

Where the information requested would mean disclosing information that identifies another individual, the SAR will be refused wholly or partly unless:

- The other individual consents to the disclosure.
- It is reasonable to comply with the request without the other individual's consent.

The DPO will determine on a case-by-case basis whether it is reasonable to comply without the other individual's consent. Considerations will include:

- Information the person making the request may have, or may get hold of, that could enable them to identify another individual referred to.
- Whether names can be deleted, or documents edited, so that information on another individual is not included, while still complying with the request.
- The type of information that would be disclosed, e.g. if it is of a sensitive nature, if it is already known or generally available to the public.
- Any duty of confidentiality owed to the other individual.
- Any steps taken to try to get the other individual's consent.
- Whether the other individual is capable of giving consent.
- Any stated refusal of consent by the other individual.

Education data

Education data is personal data which consists of information that forms parts of a student's educational record and is not data concerning health. Most of the personal information held by the college about a particular student will typically be considered to form part of the student's educational record, including a statement of SEN. Information that teaching staff keep solely for their own professional use will not form part of a student's educational record.

Child abuse data

Child abuse data is personal data consisting of information about whether the data subject is, or has been, the subject of, or may be at risk of, child abuse. This includes physical injury to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18. The college is exempt from providing child abuse data in response to a SAR from someone:

- With parental responsibility for an individual aged under 18.
- Appointed by a court to manage the affairs of an individual who is incapable of managing their own affairs.

The exemption will only apply to the extent that complying with the request would not be in the best interests of the student.

Health data

Health data will not be disclosed in response to a SAR, unless:

- Within the last six months the college has obtained an opinion from the appropriate health professional that the serious harm test for health data is not met; the appropriate health professional will also be reconsulted if it would be reasonable given the circumstances.
- The college is satisfied that the individual it is about has already seen, or knows about, the health data.

Exam scripts and exam marks

Students do not have the right to copies of their answers to exam questions but can access the information recorded by the person marking the exam. Where a student makes a SAR for this information before the results are announced, special rules will apply for how long the college has to comply with the request. The information will be provided within five months of receiving the request, or 40 days of the exam results being announced if this is earlier.

9. Record keeping

All requests will be recorded on the college's SAR Log upon being received, and updated as appropriate. Each entry will document:

- The date the SAR was received.
- The data subject's name and address.
- The name of the requester, if made on another individual's behalf.
- The type of personal data requested.
- The deadline for responding.
- Whether a charge will be made for the response.
- The reason why a request has been refused, where applicable.

10. Monitoring and review

This guidance will be reviewed on the same cycle as the Data Protection Policy by the DPO and the Principal.

Appendix 3

Carmel College

Subject Access Request (SAR) form

A subject access request (SAR) is a request made by, or on behalf of, an individual for the information which they are entitled to ask for under Article 15 of the UK GDPR. This includes personal data and other supplementary information, such as the reason for the college processing the data.

This form is intended to help individuals exercise this right. Hard copies of the form can be requested from the College Executive Coordinator or DPO or Deputy DPO. **SARs do not have to be made via this form and can also be made by other means, e.g. verbally, by letter or email.** Further information about the right of access is available at https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/.

Personal data about a student belongs to that student, and not the student's parents. For a parent to make a SAR in respect of their student the college will consider whether the student is mature enough to understand their rights. The college will determine this on a case-by-case basis.

In order to respond to a SAR, the college must be assured of the requester's identity. The college may ask for two forms of identification, e.g. a passport and proof of address. The college will respond to a SAR within one calendar month of receipt unless an extension is necessary in line with the UK GDPR. Where a SAR is refused in line with the UK GDPR, an explanation will be provided in writing and information provided on the next steps the requester may take in seeking to access the information.

Subject Access Request (SAR) Form – Carmel College	
Requester information	
Name	
Address	
Email address	
Contact number (if required)	
Preferred format of response – e.g. by email, post or verbally.	
Additional needs – Specify if you have any relevant additional needs, e.g. visual impairment, that the college will need to understand to be able to respond in an accessible format. Leave this section blank if not.	
Date	
Request on behalf of another individual (Leave this section blank if you are requesting your own personal information)	
What is the name of the individual whose information you are requesting to access?	
What is your relationship to the individual?	
What evidence do you have to confirm you are legally authorised to access the information, e.g. letter of authority, proof of parental responsibility?	

Information being requested	
Details of the personal information you wish to access – Be as specific as possible to ensure relevant information is provided, e.g: • Your staff personnel file • Your student behaviour record • Emails between 'Teacher A' and 'Teacher B' • CCTV footage at 'Location A'.	
Time period – Provide a date range for the information you are requesting, and specific times, if applicable.	
Reason for requesting this information – You are not required to provide a reason; however, it can help the college to provide the specific information you want as soon as possible.	
Additional details – Provide any additional details you think may be relevant to the request and may help the college to find the information.	

Attention: Data Protection Officer
HR
Carmel College
Prescot Road
St. Helens
Merseyside
WA10 3AG

Email: hr@carmel.ac.uk

The information you provide on this form will be used to process your request. Summary information may be retained for statistical or audit purposes. By providing this information you consent to Carmel College storing your information for these purposes. Carmel College will process your data in accordance with the General Data Protection Regulation.

Appendix 4

Personal data breach record

A personal data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Under the UK GDPR, data controllers are required to always document any personal data breaches they are aware of. The record must include the facts of the breach, its effects and the remedial action taken. Colleges can use this template to record any data breaches.

This form should be completed by the DPO, and they should confer with all the individuals involved to ensure that all information recorded in the form is correct. The college can use this form as their own personal record of a data breach. Any information within this form can be used to improve the college's data protection provisions and policies. The form should be reviewed and updated as necessary if additional information comes to light, e.g. concerning who has had access to the personal data or the consequences of the breach.

Colleges must also notify the ICO of a breach within 72 hours of becoming aware of it, using an online form if it is likely to result in a risk to the rights and freedoms of individuals. If the data breach is the result of a cyber-security incident, this should also be reported to the National Cyber Security Centre.

Personal data breach record

Breach overview	
Date and time breach happened	
Data and time breach discovered	
Type of data breach	**[Identify the nature of the breach, e.g. disclosed in error, unauthorised access, lost in transit, stolen hardware.]**
Groups of data subjects affected	**[Indicate whose data has been breached, e.g. staff, students, parents.]**
Approximate number of data subjects affected	
Description of personal data included in the breach	
Breach details	
What has happened?	
How did the breach occur?	
How was the breach discovered?	
What preventative measures were in place?	
Breach consequences and response	
What is the impact of the breach?	
Is there likely to be a high risk to individuals' rights and freedoms?	**[This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data**

	have been breached. Explain the reasoning.]
Is the personal data concerned considered to be contained and the risk to data subjects mitigated?	**[Consider, for example, if any lost data has been located, who has access to it, if it is encrypted or password protected, if it has been returned or securely disposed of.]**
Has the ICO been notified of the breach?	**[Indicate whether the ICO has been notified and record the reason for the decision.]**
What information have individuals affected by the breach been given?	
What remedial action has been taken?	

Date record completed	
Name of DPO	
DPO signature	