Data Protection Policy & Code of Practice

March 2024

Version 4

Approved by the Finance and Resources Committee 13th March 2024

Review date March 2027

Contents

1. INTRODUCTION

This is a statement of Data Protection Policy adopted by Hugh Baird College Further Education Corporation.

Hugh Baird College needs to collect and use certain types of information about people with whom it deals in order to operate. This includes current, past and prospective students, employees, suppliers and others with whom it communicates. In addition, the College is required by law to collect and use certain types of information to comply with statutory legislation and the requirements of its funding providers. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer or recorded on other material – and that there are safeguards to ensure compliance with the General Data Protection Regulation (GDPR).

The GDPR lays down rules relating to the protection of individuals with regard to the processing of personal data and is designed to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Hugh Baird College regards the lawful and correct treatment of personal information as very important to its successful operation and to maintaining confidence between those with whom it deals and the College itself. The College ensures that treats personal information lawfully and correctly.

To this end, the Corporation sets out to fully adhere to article 6 of the GDPR which lays down the six legal bases concerning the lawfulness of data processing, which are detailed on page 4 of this document.

The GDPR covers all Personal Data that is held automatically, including word-processed documents, databases and e-mails. It also extends to Personal Data held in manual records where these can be accessed by reference to a person.

The GDPR requires the College to notify the Information Commissioner of the types of Personal Data that it holds, the categories of individuals for which it holds this information, to whom it may be disclosed and the purposes for which Personal Data is processed. It also requires the College to confirm if it transfers Personal Data worldwide. The College is further obliged to inform the Information Commissioner's Office within 72 hours of any breaches of the GDPR that it may become aware of.

All members of the College have a duty to ensure compliance with the GDPR.

2. DEFINITIONS

The following is a list of definitions used within this Policy:

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

"Data" means any information being processed using equipment operating automatically in response to instructions given for that purpose and that has been recorded with the intention that it should be processed by means of such equipment or is recorded as part of a Relevant Filing System.

"Data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Data Controller" means an individual who determines the purpose for which or the manner in which any Personal Data is or is to be processed. It also extends to a person who gives instructions about the use of Personal Data even though it may not come into their possession.

"Data Processors" means any person other than an employee of the Data Controller who processes Data on behalf of the Data Controller. This would include people such as market researchers who collect Personal Data on behalf of the Data Controller.

*"**Data Subject**"* means an identifiable or identified living individual who is the subject of the Personal Data. A Data Subject could be anywhere in the world but must be living.

"GDPR" means the General Data Protection Regulation

"Personal Data" means Data which relates to a living individual who can be identified from that Data or from that Data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about that individual and any indication of the Data Controller or any other person's intentions towards that individual. The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

"Processing" means organising, adapting and altering Data, retrieving, consulting or using the Data, disclosure of the Data in any way, aligning, combining, blocking or erasing Data. The definition is so wide that it would include someone looking at a computer screen.

"Relevant Filing System" means any set of information relating to individuals which is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible even where Processing does not take place automatically. This would include any paper files relating to an individual student.

"Sensitive Personal Data" means Personal Data about a Data Subject which relates to sensitive issues such as their racial or ethnic origin, their political opinions, religious or other similar beliefs, membership of a trade union, physical or mental health or condition, sex life, commission or alleged commission by them of any offence or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings and the Court's sentence in such proceedings.

3. GDPR - THE SIX LEGAL BASES FOR PROCESSING DATA

The GDPR sets down the six legal bases for the processing of personal data. Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. processing is necessary for compliance with a legal obligation to which the controller is subject;

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5. 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;

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. DATA PROTECTION PRINCIPLES

In keeping with core themes of the data protection principles in GDPR (Article 5) the College shall ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimisation principle");
- Accurate and where necessary kept up to date (the "accuracy principle");
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle");
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

5. PROCEDURE

This Code of Practice is intended to assist everyone within the College to comply with the GDPR. The College as a Data Controller will hold the minimum Personal Data necessary to enable it to perform its functions, and the data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without undue delay. The College will provide to any individual who requests it, (in a manner specified by the GDPR a formal reply to all enquiries made by that individual in accordance with the rights of Data Subjects).

It is the responsibility of every employee of the College to ensure compliance with not only this Code of Practice but the GDPR itself. The College expects all of its employees to comply fully with this Code of Practice and the Act when processing Personal Data as part of their employment or studies at the College.

6. RESPONSIBILITIES

Overall responsibility for compliance with the GDPR lies with the College Corporation. Managerial responsibility is exercised by the Data Protection Officer.

If this policy does not provide guidance on a particular issue, the query should be directed to the Data Protection Officer.

Data Protection Officer

The Data Protection Officer for Hugh Baird College is:

Matt Larkin

Vice Principal – Finance and Corporate Services

Tel: 0151 353 4423

E-mail: matt.larkin@hughbaird.ac.uk

All employees have a general duty to observe the GDPR, any specific instructions given by the College and any College Codes of Practice, Policy or procedures relating to the GDPR. It is the responsibility of each employee to assist the Data Protection Officer to maintain compliance with the GDPR in the relevant area. Employees should not disclose Personal Data that comes into their possession to other people within the College unless this is necessary to perform their duties.

7. NOTIFICATION

The GDPR requires the College to notify the Information Commissioner of the ways in which it processes Personal Data. Failure to notify the Information Commissioner is a criminal offence. The College's notification must be renewed annually. However the notification should be amended whenever necessary. It is the responsibility of all employees to ensure that any processing of Personal Data that they undertake is within the terms of the College's notification. If you believe that any processing which you intend to carry out falls outside of the College's current notification, you must inform the Data Protection Officer. You should not carry out the intended processing until the Data Protection Officer (or nominee) confirms that it will be covered by the College's notification.

The College is only able to process Personal Data within the terms of its notification. If the College processes Personal Data outside of its notification, both it and the individual processing the data may incur civil and criminal liability. The notification will be made by the Data Protection Officer, after confirmation as to the details have been received.

You can obtain details of the College's current notification from the Data Protection Officer.

8. INTERNAL REGISTRATION

Detailed records of all computerized personal data and structured manual data files retained by the College will be held by the Data Protection Officer who will carry out an annual audit to ensure compliance with the College's Data Protection Policy and the GDPR.

9. EXEMPTIONS

Exemptions include matters such as National Security, Crime and Taxation and Health matters. These exemptions that in certain cases allow the College to disclose data without consent are dealt with in the section of this Code of Practice that relates to the disclosure of Personal Data.

The guidelines issued by the office of the Information Commissioner set out all exemptions from the GDPR. These can be viewed on their website at:

http://ico.org.uk/

10. ACCESS TO PERSONAL DATA

Access to Personal Data includes disclosures and Subject Access requests.

Disclosure of Personal Data is permitted under the GDPR where the College has both notified the usage to the Information Commissioner and complied with the requirements of the legal bases for processing. It is essential that at the time the data is collected Data Subjects are informed of the purposes for which it will be used and the individuals or organisations to whom it may be disclosed. If it is proposed to use the information obtained for direct marketing purposes, Data Subjects should be informed of this purpose at this time and given the opportunity to decline this usage of the data.

Within the terms of the GDPR the following are authorised persons to whom Personal Data may be disclosed:

- the Data Subject, or someone acting on behalf of the Data Subject;
- a third party at the request or with the consent of the Data Subject, or of someone acting on behalf of the Data Subject;
- a third party contact nominated by the Data Subject and notified to the College as the person to be contacted in the case of an emergency.

Within the terms of the GDPR, Personal Data may only be disclosed where the purposes have been notified to the Information Commissioner and where the Data Subject's informed consent has been obtained. When data is used for the purpose of direct marketing care must be taken to ensure that the Data Subject has not objected to this processing either at the date of collection or at a later date.

Within the terms of the GDPR the following are purposes where data may be disclosed to third parties **without** the consent of the Data Subject:

- for legal purposes, if the Personal Data is required by statute, rule of law or Court Order; is required to obtain legal advice; or required for legal proceedings in which the person making the disclosure is a party or witness;

- to safeguard national security based on a certified request from a Cabinet Minister, Attorney General or Lord Advocate;

- for the prevention of crime and for taxation purposes. Disclosures for these reasons will only occur if the College is satisfied as to the purpose of such a request and the likelihood of substantial prejudice if the request was refused;

- to protect the vital interests of the Data Subject;

- to carry out regulatory functions such as securing the health, safety and welfare of persons at the College.

It should be remembered that requests for disclosure for the purposes listed above should be considered on a case by case basis only and that the Data Protection Officer should be consulted when necessary. Any decisions made to disclose data in accordance with the above purposes should be fully documented.

Responding to Disclosure Requests

All requests for disclosure of Personal Data from persons outside the College must be treated with caution by all staff. The College must ensure that procedures are in place to provide adequate safeguards against disclosure to unauthorised persons and/or for unauthorised purposes within their relevant area and should take account of the following guidelines:

- Personal Data must not be disclosed to an external body over the telephone. Individuals making such enquiries should be asked why the information is required and be informed of the College's requirement to comply with the GDPR. Wherever possible the Data Subject should be informed of the enquiry to enable them to respond directly.

- Parents, relatives and guardians should be informed of the College's requirement to comply with the GDPR if making representation on behalf of an employee.

- Personal Data requested by members of staff from other areas of the College should only be released when it has been established that the information required is necessary for them to carry out their official duties.

- All requests from outside agencies such as the Police, DWP, Inland Revenue, Local Authorities Overseas Embassies or High Commissions should be submitted in writing and forwarded to the Data Protection Officer.

Subject Rights

The GDPR gives certain rights to individuals in respect of Personal Data held about them by others. These rights include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subject to automated decision-making;
- the right to data portability

The Data Subject has the right to prevent processing likely to cause damage or distress; the right to prevent processing for the purposes of direct marketing; the right to be informed of the logic behind any automatic decision making; the right to take action for compensation if they suffer damage by any contravention of the GDPR by the Data Controller; the right to take action to rectify, block, erase or destroy inaccurate data and finally the right to ask the Commissioner to assess whether or not it is likely that any processing of Personal Data has not been carried out in accordance with the Act. The Data Subject may also exercise his/her right withdraw consent and to be forgotten, meaning that the Data Controller must safely dispose of all records relevant to the Data Subject.

Subject Access Requests

Data Subjects have the right to be informed whether Personal Data about them is being processed by the College and the right to receive a copy of that Personal Data together with details of the purpose for which it is being processed and to whom the data might be disclosed within one calendar month of making that request. This entitlement relates to all Personal Data held about an individual, whether in computerised records or in a manual file.

A Subject Access request must be in writing which includes email, but does not have to specifically refer to Subject Access, Data Protection or the GDPR. An individual could ask for all information that the College holds about them.

All requests for Subject Access must be immediately passed to the Data Protection Officer.

The Data Protection Officer will co-ordinate the formal reply to the applicant, or will advise them that no Personal Data relating to them is held.

Responding to Subject Access Requests

Certain rules must be followed by the data user when retrieving Personal Data in response to a Subject Access Request. These are that:

- the data need not necessarily be provided as a print-out. The Data Controller may choose to write or type the data to be supplied, with any accompanying explanation;

- the data must be intelligible to the Data Subject;

- the data given need only be that available at the time the request was received, however, it can differ as routine updates of data can continue between the dates of the receipt of the request and the end of the retrieval process;

- having received a request, NO SPECIAL AMENDMENTS OR DELETIONS OF DATA CAN BE MADE WHICH WOULD NOT OTHERWISE HAVE BEEN MADE;

- if Personal Data includes information which identifies another individual, (and was not originally provided by the Data Subject) the consent of the third party should be sought before the disclosure is made. If the third party does not consent to this disclosure the information may be edited out of the reply to the Data Subject providing the third party remains unidentifiable. Third party data should not be edited out completely - for example, they may be redacted but with X and Y being used instead of full names;

- if data retrieved is used to make an automatic decision which may significantly affect the Data Subject, an explanation must be provided of the logic underlying the decision making process.

The formal procedure for controlling and processing Subject Access Requests is cumbersome. Wherever possible, the informal disclosure of Personal Data to Data Subjects is encouraged, particularly where administrative gains may result - for example, for the periodic confirmation of the accuracy of personal details, such as current address and so on.

Where an informal approach is adopted, it is essential that the Data Protection Principles and College's procedures are fully observed. Specifically, Personal Data should only be made available to the Data Subject, and if transmitted in the internal mail system, should be in a sealed envelope marked "Confidential - for the attention of 'the Data Subject'.

Prevention of Processing

A Data Subject is entitled to request that the College either ceases or does not begin to process information that the Data Subject considers may cause unwarranted substantial damage or distress to them or another. These requests must be received in writing from the individual and should be forwarded to the Data Protection Officer.

After an acknowledgement letter is sent to the applicant, the Data Protection Officer will forward a copy of the request, if necessary, to the relevant Director requiring that they consider the application and make a decision whether or not to continue processing based on all the relevant circumstances of the case. The Data Protection Officer will, within one calendar month of the original request being received, send a written reply to the individual setting out the Director's decision to either comply with the request, or to explain the reasons why the College feels that the request is unjustified. If the decision taken is to cease processing the Data, the relevant Director will immediately take steps to comply with this action.

11. SECURITY

Under the GDPR security measures apply not only to the security of computer hardware and storage media, such as discs and USB pens, but also to source documents, manual records, printouts and oral disclosure. Security measures are also applicable throughout the use and processing of Personal Data, including the handling, transmission, disclosure and disposal of documents containing Personal Data. The College's procedures outlined in this document have incorporated security measures.

The Directors are responsible for ensuring that adequate security arrangements for Personal Data exist within their relevant areas. Although this responsibility may be delegated, it is incumbent on the Directors to ensure that staff in their area are aware of their responsibilities with regard to Data Protection.

The GDPR gives specific guidelines on the "appropriateness" of security regulations. These should be observed when developing procedures to support the College's Data Protection responsibilities.

In terms of physical security, the following guidelines apply:

- access to buildings/rooms containing computer hardware must be controlled;
- adequate precautions must be taken against burglary, fire or natural disaster;
- casual passers-by or other unauthorised personnel should not be able to read data off screens or printouts;
- screen savers should be used in all cases;
- back-up copies of data should be stored separately from live files;

- manual documents from which Personal Data are extracted must be properly secured and kept in locked storage when not in use;

- printed material containing information extracted from Personal Data must be handled and disposed of correctly.

In terms of software and where security measures are programmed into systems:

- the use of global passwords is discouraged. Passwords should be known only to a minimum number of authorised persons and should be changed at regular intervals;

- individual passwords must be closely safeguarded and not divulged to others. They should be changed at regular intervals;

- full use should be made of facilities to restrict access on the basis of authority levels;

- discs and USB pens on which Personal Data are recorded must be securely safeguarded and accounted for.

Specific regulations apply to individuals who use the computing facilities of the College. These regulations are contained in the College's ICT Policies for Staff.

When using third party agencies to process Personal Data on behalf of the College a written contract should be entered into requiring that the Act is complied with at all times.

Processing of Data Off-Campus (including Remote Access)

Extra vigilance is required when personal data, which has been gained by virtue of employment at the College, is processed off campus. Personal Data can only be taken or processed off campus if the following criteria are met:

- the Personal Data is used or processed in accordance with the duties of the member of staff and for no other purpose;

- the processing activities are in accordance with this Policy and Code of Practice; in this respect the security measures outlined above must be strictly complied with both on or off the campus;

- the Personal Data must be stored off campus for the minimum time required and then disposed of in a secure manner.

- off-site computer equipment should be sufficiently secure to prevent unauthorised access and data corruption.

12. TRANSFER OF DATA OUTSIDE THE EEA

The College is prohibited from transferring personal data outside the European Economic Area to a third country that does not have adequate data protection. The European Commission has the power to approve particular countries as providing an adequate level of data protection, taking into consideration the data protection laws in force in that country and its international commitments. The current list of "approved countries" is as follows:

Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay

13. DATA PROTECTION AND EMAIL

Personal Data includes any Personal information stored in email messages and, potentially, email addresses themselves. Staff must therefore comply with this Policy and Code of Practice in relation to any Personal Data which is sent, received or stored in the form of an email.

14. DATA PROTECTION AND THE INTERNET

The provisions of the Data Protection Act apply equally to processing on the World Wide Web as they do to processing on all other information systems. When Personal Data is requested by the College on a website the following information must be supplied to the Data Subject:

- the purpose for which the data is collected;
- the description of the organisations or individuals to whom the data might be disclosed;
- the details of any direct marketing for which the data might be used together with the opportunity for the individual to object to this use of the data;
- a statement regarding the security of the internet as a mode of communication.

When Personal Data is obtained from the website of another organisation, the relevant Director must ensure that the subsequent use of the Personal Data conforms to the information provided to the Data Subject. If any further subsequent use of this data is proposed that was not disclosed at the time of collection, consent must be obtained from the Data Subject before commencing this processing.

Any Personal Data which is placed on a website is treated as data which is transferred outside the EEA. Written informed consent will be obtained from all staff before details are entered on the College's site. Further guidance on Data Protection issues is available from the following websites:

The office of the Information Commissioner at:

http://ico.org.uk/

The JISC Code of Practice for HE and FE Sectors at:

http://www.jisc.ac.uk

Guidelines for Retention of Personal Data

The guidelines outlined in Appendix 1 below (although not exhaustive) should be considered in relation to all retention / disposal of data.

Appendix 1 – Guidelines for the Retention of Personal Data

Type of Record	Suggested Retention Period	Reason for Length of Period
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	Potential litigation.

Wages and salary records	6 years	Taxes Management Act 1970
DBS details	6 months from the date of receipt	DBS guidance
Application forms and interview notes	At least 6 months from the date of the interview	Time limits on litigation
Facts relating to redundancies where less than 20	3 years from the date of redundancy	As above
Facts relating to redundancies where 20+	12 years from the date of redundancy	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 3 years after the end of the financial year to which the records related	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records related	Statutory Sick Pay (General) Regulations 1982
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health Records in general	During employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
Disciplinary Records	3 years	Recommended by BSI

Staff appraisal records and staff references	5 years	Recommended by BSI
Data relating to educational contracts	7 years / In keeping with any agreement within the contract	Contractual obligation
Student records, including records of academic achievements and conduct. For exam results a retention period of 10 years should be applied. A retention period of three years for all other records should be applied.	At least 7 years from the date of leaving in cases where there is litigation for negligence. At least 10 years for personal academic references, *with the agreement of the student*	Limitation period for negligence

Appendix 2 – Procedures to be followed in case of a suspected Data Brach

Purpose

The objective of these procedures is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definitions / Types of breach

For the purpose of these procedures, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the College's information assets and / or reputation.

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, i-Pad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;
- human error;
- offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

Any individual who accesses, uses or manages the College's information is responsible for reporting any data breach and / or information security incidents immediately to the College's Data Protection Officer, Matt Larkin, (at matt.larkin@hughbaird.ac.uk).

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

All staff should be aware that any breach of Data Protection legislation may result in the College's Disciplinary Procedures being instigated.

Containment and recovery

The Data Protection Officer (DPO)*** will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

***Where the DPO is alleged to be responsible for the breach an interim DPO, who shall be a member of the Principalship, shall be appointed for the duration of the investigation.

An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach. The DPO shall lead any investigation in conjunction with relevant staff (this will depend on the nature of the breach and the area of the College within which the breach is alleged to have taken place).

The DPO will establish who may need to be notified as part of the initial containment and will inform the police, if appropriate.

Advice from staff members across the College may be sought in resolving the incident promptly. The Head of Services, for example, would be contacted where the issue involved the College's IT infrastructure. The DPO, in liaison with the relevant staff will then determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and risk assessment

An investigation will be undertaken by the DPO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The DPO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:
the type of data involved;

- its sensitivity;
- the protections are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen);
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

Notification

The DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation2;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the College for further information or to ask questions on what has occurred.

The DPO Must consider notifying third parties such as the police, insurers or banks. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The DPO will consider whether the Marketing Department should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the College's Principalship and Governing Body.