Luccombe Hub

This document forms part of the policy handbook and is intended for use at Luccombe Hub

Title:	**UK GDPR & Data Protection Policy**
Subject Area:	General
Applies:	Immediately
Issued:	01/03/2022
Next Review:	01/03/2025
Sponsor:	Henri Monier-Williams in conjunction with SLT
Contact:	Marcus Monier-Williams
Email:	Marcus@Luccombehub.com

1. Introduction

1.1 Aims

Following the end of the transition period of the UK from the EU. The Information Commissioners Office (ICO) confirms that EU GDPR has been retained as part of the Brexit deal and incorporated into UK General Data Protection Regulation (GDPR) Law. This policy will reflect these continued obligations together with The Data Protection Act 2018 (DPA) that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

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

1.2 Consultation

The Luccombe Hub will communicate this policy to all staff, relevant professionals and learners through inductions, meetings, day to day communications, staff meetings and training. A copy of this policy and all policies will be available on request or via the website.

1.3 Legislation and guidance

Information Commissioners Office (ICO)
UK General Data Protection Regulation (GDPR)
The Data Protection Act 2018 (DPA)
The Education (Pupil Information) (England) Regulations 2005

2. Procedures and practice

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information.

The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the UK GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The Centre collects an amount of personal data every year including: learner records, staff records, names and addresses of those enquiring after places, references, fee collection as well as the many different types of data used by the Centre in line with their education and therapeutic business practices. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Principles

The principles set out in the EU GDPR and retained under the UK GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- 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 Centre.
- 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
- Processing is necessary for compliance with a legal obligation to which the data controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller.
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters.
- Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the Centre's relevant privacy notice.

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the Centre's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
    (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Centre or the data subject
    (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    (e) the processing relates to personal data which are manifestly made public by the data subject
    (f) the processing is necessary for the establishment, exercise or defence of legal claims
    (g) the processing is necessary for reasons of substantial public interest

(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
(i) the processing is necessary for reasons of public interest in the area of public health.

The Centres' privacy notice sets out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Where the Centre cannot rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the Centre can demonstrate compliance with the UK GDPR.

Data Protection Impact Assessments (DPIA)

The Centre processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) Consideration to Data Protection Impact must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Documentation and records

Written records of processing activities to be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the Centre's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The Centre should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

The Centre will issue privacy notices as required, informing data subjects (or their parents, depending on age of the learner, if about learner information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the UK GDPR including the identity of the DPO, how and why the Centre will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. The Centre will also check that the data was collected by the third party in accordance with the UK GDPR and on a basis which is consistent with the proposed processing of the personal data.

The Centre will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The Centre will issue a minimum of two privacy notices, one for learner information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

The Centre will ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the Centre no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the Centre is verifying whether it is accurate), or where you have objected to the processing (and the Centre are considering whether there are legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA if applicable.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The Centre expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not Centre staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the Centre policies).

Information Security

The Centre will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation.

The Centre will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Centre has implemented and maintains in accordance with the UK GDPR and DPA.

Where the Centre uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the Centre
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the Centre and under a written Agreement for Services.
- the organisation will assist the Centre in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the Centre as requested at the end of the contract
- the organisation will provide the Centre with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Centre immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from Henri Monier-Williams.

Storage and retention of personal information

Personal data will be kept securely in accordance with the Centre's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.

Personal information that is no longer required will be deleted.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The Centre must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The Centre must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform Centre Lead immediately that a data breach is discovered and make all reasonable efforts to recover the information.

Consequences of a failure to comply

The Centre takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Centre and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the Centres procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

2.3 Aspects

The Centre as the Data Controller will comply with its obligations under the UK GDPR and DPA. The Centre is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines for serious breaches of the UK GDPR, therefore it is imperative that the Centre and all staff comply with the legislation.

3. Concluding notes

3.1 Monitoring and review

This policy will be reviewed on a three yearly basis unless otherwise earlier due to changes in guidance and law. Data held by The Luccombe Hub will be audited annually.

3.2 Links to other policies

3.3 Appendices

Appendix 1 – Procedure for Access to Personal Information

1. Right of access to information

There are two distinct rights of access to personal information held by Centre.

Under the UK GDPR and the Data Protection Act 2018 an individual (e.g. learner, parent or member of staff) has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see explanation below).

The Education (Pupil Information) (England) Regulations 2005 gives parents the right of access to curricular and educational records relating to their child.

2. Processing a request

Requests for personal information must be made in writing and addressed to the Henri Monier-Williams. If the initial request does not clearly identify the information required, then clarification should be sought.

The identity of the requestor must be verified before the disclosure of any personal information, and checks should also be carried out regarding proof of relationship to the child.

Evidence of identity can be established by requesting production of the following (this list is not exhaustive):

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

Individuals are entitled to be told if we are processing their personal information, obtain a copy of that information and other supplementary information – see below.

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes for processing their data;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

Information can be viewed at the Centre with a member of staff on hand to help and explain matters if requested or provide a face to face handover.

The views of the applicant should be taken into account when considering the

method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

3.Information relating to children

Children have the same rights of access to their own personal information as adults, and the same rights of privacy. There is no minimum age in English law, however current practice accepts that, provided a child is mature enough to understand their rights, a child of, or over the age of 13 years shall be considered capable of giving consent. This does not rule out receipt of a valid request from a child of a younger age, as each request should be considered on its merits on an individual basis.

When a subject access request is received from a child it will need to be judged whether the child has the capacity to understand the implications of their request and of the information provided as a result of that request. If the child does understand then their request will be dealt with in the same way as that of an adult.

If a parent or legal guardian makes a request on behalf of a child age 13 and over the request will only be complied with when assurances are received that the child has authorised the request and that their consent was not obtained under duress or on the basis of misleading information. If the child does not understand, then a request from a parent or legal guardian for the child's information will only be complied with when assurances are received that they are acting in the best interests of the child.

4.Response time

UK GDPR & DPA

The response time for compliance with a subject access request is **one month** following date of receipt. The timeframe does not begin until the Centre has received all the information necessary to comply with the request i.e. proof of identity.

The timeframe may be extended by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Education Regulations

Requests for information from parents for access to information classed as being part of the education record must be responded to within **15 Centre days.**

5. Charges

Under UK GDPR & DPA:

Should the information requested be personal information that **does not** include any information contained within educational records the Centre cannot make a charge, unless the request is manifestly unfounded or excessive. You may charge a "reasonable fee" for the administrative costs of complying with the request.

The Centre can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies.

Under the Education Regulations

The Centre may make a charge if the information requested relates to the educational record, the amount charged will depend upon the number of pages provided. The fees work on a sliding scale basis as below.

Number	Maximum
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-69	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

6. Exemptions

There are some exemptions to the right to subject access that apply in certain circumstances or to certain types of personal information. **This means all information must be reviewed prior to disclosure**.

Included below are some of the exemptions that apply to a Centre, this is not an exhaustive list;

Third Party information: If the information held identifies other people, then it will sometimes be right to remove or edit that information so as not to reveal the identity of the third parties, unless the third parties have agreed to the disclosure. (This is less likely to apply to information identifying teachers or other professionals unless to disclose it would cause them serious harm.) Reasonable steps must be taken to obtain third party consent to disclosure. If the third parties cannot be located or do not respond it may still be reasonable to consider disclosure if the information is of importance to the data subject. The Centre must still adhere to the **one month** statutory timescale.

Where redaction (information edited/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, meaning any codes or technical terms will need to be clarified and explained. If information contained within the

disclosure is difficult to read or illegible, then it should be retyped.

Information likely to cause serious harm or distress: Any information which may cause serious harm to the physical or mental

health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

Crime and Disorder: If the disclosure of the information is likely to hinder the prevention or detection of a crime, the prosecution or apprehension of offenders, or the assessment or collection of any tax or duty, the information should be withheld.

Legal professional privilege: If the information is general legal advice or advice which relates to anticipated or pending legal proceedings it is subject to 'legal professional privilege'. The disclosure of any communication to or from a legal advisor to another person (including the data subject) should not take place unless this has first been discussed with the legal advisor concerned.

References: The right of access does not apply to references given (or to be given) in confidence.

Absence of or invalid consent to disclosure: If the data subject is considered incapable of giving valid consent to disclosure (i.e. they do not have the capacity to understand the nature/implications of the access request), or if it is suspected that the consent was obtained under duress by someone acting on their behalf, or based on misleading information, then access should be refused.

7. Complaints

Complaints about the above procedures should be made to the Data Protection Officer (DPO) – Henri Monier-Williams who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Centre's complaint procedure.

Complaints which are not appropriate to be dealt with through the Centre's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

8. Contacts

Further advice and information can be obtained from the Information Commissioner's Office: www.ico.gov.uk