Overarching GDPR Policy and Procedure

Purpose

The purpose of this policy is to ensure that The Greenhouse understands the key principles of UK GDPR.

This policy sets out the steps that need to be taken by The Greenhouse to ensure that The Greenhouse handles, uses and processes personal data in a way that meets the requirements of UK GDPR. It should be read alongside the suite of UK GDPR policies, procedures and guidance The Greenhouse.

This policy applies to all staff at The Greenhouse who process personal data about other staff, Learners and any other living individuals as part of their role.

To meet the legal requirements of the regulated activities that The Greenhouse is registered to provide:

- General Regulations for Approved Centres (JCQ)
- Awarding Organisation Requirements
- UK GDPR (as defined in section 3(11) Data Protection Act 2018
- The Data Protection Act 2018

Scope

The following roles may be affected by this policy:

- All staff

The following Learners may be affected by this policy:

- All Learners

The following stakeholders may be affected by this policy:

- Employers
- Awarding Organisation
- Bluestones Medical Complex Care
- Awarding Organisations

- Department of Education

Objectives

The objective of this policy is to ensure staff have a working knowledge into the principles and requirements of UK GDPR.

Alongside the suite of policies, procedures and guidance available, The Greenhouse can demonstrate that appropriate steps are taken to ensure it complies with UK GDPR when handling and using personal data provided by both staff and learners.

This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

This policy will assist with understanding the obligations of The Greenhouse in respect of the rights of the staff and Learners who have provided personal data and the steps The Greenhouse should take if there is a personal data breach.

Policy

GDPR Background

GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998.

Following the UK's departure from the EU, UK GDPR was incorporated into domestic law that applies in the UK.

UK GDPR provides greater protection to individuals and places greater obligations on organisations than the pre GDPR data protection regime but can be dealt with in bite-size chunks. Compliance with data protection laws should enhance service provision and care provided by engendering trust between The Greenhouse and it's learners.

All staff must ensure the ways in which they handle personal data meet the requirements of UK GDPR.

The Approach of The Greenhouse to UK GDPR

The Greenhouse is required to take a proportionate and appropriate approach to UK GDPR compliance. The Greenhouse understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. The Greenhouse understands that if significant volumes of personal data are processed, including special categories of personal data, or it has unusual or complicated processes in place in terms of the way personal data is handled, The Greenhouse will consider obtaining legal advice specific to the processing conducted and the steps that may need to be taken.

UK GDPR and the Data Protection Act 2018 do not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

Process for Promoting Compliance at The Greenhouse

To ensure The Greenhouse complies with UK GDPR and the Data Protection Act 2018, a suite of data protection policies and resources are available and should be read in conjunction with this overarching policy to provide a framework for compliance.

Overview of Key Terms, Key Principles and Documents

The key principles and themes of each of the documents listed above are summarised below:

Key Terms

UK GDPR places obligations on all organisations that process personal data about a data subject. A brief description of those three key terms is included in the

Definitions section of this document and is expanded upon in the Key Terms Guidance.

The requirements that The Greenhouse needs to meet vary depending on whether The Greenhouse is a controller or a processor. In most cases The Greenhouse will be a controller. The meaning of 'controller' and 'processor', together with the roles they play under UK GDPR, are explained in the Key Terms Guidance. The Greenhouse understands that it may be a controller in some circumstances and a processor in others.

Special categories of data attract a greater level of protection, and the consequences for breaching UK GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This information is also covered in more detail in the Key Terms Guidance.

Key Principles

There are 7 key principles of UK GDPR which The Greenhouse must comply with. They are:

- Lawful, fair and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring that the personal data is adequate and relevant
- Ensuring that the personal data is accurate
- Ensuring that the personal data is only retained for as long as it is needed
- Ensuring that the personal data is kept safe and secure
- Accountability - taking responsibility for what you do with personal data and how you comply with the other principles

The Greenhouse must have appropriate measures and records in place to be able to demonstrate compliance.

These key principles are explained in more detail in the guidance entitled 'UK GDPR – Key Principles'. The Greenhouse recognises that, in addition to complying with the key principles, it must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance.

The Greenhouse understands that a 'privacy by design' approach must be adopted. This means that data protection issues should be considered at the very start of a project, or engagement with a new Learner. Data protection should not be an after-thought.

These ideas are also covered in more detail in the Key Principles Guidance.

Processing Personal Data

The provision of health or social care or treatment or the management of health or social care systems and services is expressly referred to in UK GDPR as a lawful basis upon which an organisation is entitled to process special categories of data. In terms of other types of personal data, The Greenhouse must only process personal data if it is able to rely on one of a number of grounds set out in UK GDPR.

The grounds which are most commonly relied on are:

- The data subject has given their consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract with the data subject; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the data subject or another living person
- The processing is necessary to perform a task carried out in the public interest

The grounds set out above are explained in more detail in the guidance entitled 'UK GDPR – Processing Personal Data'.

Data Protection Officers

The Greenhouse understands that some organisations will need to appoint a formal Data Protection Officer under UK GDPR (a 'DPO'). The DPO benefits from enhanced employment rights and must meet certain criteria, so it is recognised that it is important to know whether The Greenhouse requires a DPO. This requirement is outlined in the Appointing a Data Protection Officer Policy and Procedure.

Whether or not The Greenhouse needs to appoint a formal Data Protection Officer, it will appoint a single person to have overall responsibility for the management of personal data and compliance with UK GDPR.

Data Security and Retention

Two of the key principles of UK GDPR are data retention and data security.

- Data retention refers to the period for which The Greenhouse keeps the personal data that has been provided by a data subject. At a high level, The Greenhouse must only keep personal data for as long as it needs the personal data
- Data security requires The Greenhouse to put in place appropriate measures to keep data secure

These requirements are described in more detail in the Data Security and Data Retention Policy and Procedure.

Website Privacy and Cookies Policy and Procedure

Where The Greenhouse collects personal data via a website, it understands that it will need a UK GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy is provided.

Wider Privacy Policies

The Greenhouse understands that it is required to provide certain information to all individuals about whom it processes personal data, and that such information is

usually provided via privacy policies. A template external and employee-facing privacy policy is provided.

The template privacy policy sits alongside a consent form which can be used to ensure that The Greenhouse obtains appropriate consent, particularly from the Learner, to the various ways in which The Greenhouse uses the personal data (where consent is the most appropriate ground for The Greenhouse to rely upon). The consent form contains advice and additional steps to take if the Learner may lack capacity.

Subject Access Requests

One of the key rights of a data subject is to request access to, and copies of, the personal data held about them by an organisation. Where The Greenhouse receives a subject access request, it understands that it will need to respond to it in accordance with the requirements of UK GDPR. To help staff at The Greenhouse understand what a subject access request is and how they should deal with a subject access request, a Subject Access Requests Policy and Procedure is available to staff. A process map to follow when responding to a subject access request, as well as a subject access request letter template is also included.

The Rights of a Data Subject

In addition to the right to place a subject access request, data subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by The Greenhouse. Not all rights apply in all circumstances. Rights of the data subject are covered in detail in the corresponding guidance.

Breach Notification Under UK GDPR

In certain circumstances, if there is a personal data breach (i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data), the ICO must be notified and potentially any affected data subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to

all staff, together with a process map for The Greenhouse to follow if a breach of UK GDPR takes place is available.

Transfer of Data

If The Greenhouse wishes to transfer personal data to a third party, an agreement must be put in place to set out how the third party will use the personal data. If the third party is processing data on the instruction of The Greenhouse, the contract must cover specific points set out in UK GDPR. Bluestones Medical Complex Care (EQ) must consider carrying out due diligence investigations on third party recipients of personal data of which The Greenhouse is the controller.

Data Protection Impact Assessments

The Greenhouse must carry out Data Protection Impact Assessments each time it processes personal data in a way that presents a 'high risk' for the data subject. Examples of when a Data Protection Impact Assessment should be conducted are provided in the relevant policy and procedure.

Compliance with GDPR

The Greenhouse understands that there are two primary reasons to ensure that compliance with UK GDPR is achieved:

- It promotes high standards of practice and learning and development, and provides significant benefits for staff and, in particular, learners.
- Compliance with UK GDPR is overseen in the UK by the ICO. Under UK GDPR, the ICO has the ability to issue a fine of up to £17.5 million or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences of non-compliance are therefore significant.

The Greenhouse appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance and offers guidance to organisations about how to comply. A one-off, minor breach may not attract the attention of the ICO but if The Greenhouse persistently breaches UK GDPR or commits significant one-off

breaches (such as the loss of a large volume of personal data, or the loss of special category personal data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of The Greenhouse and its data protection policies and processes and to issue instructions for The Greenhouse to comply or put right its data processing practices including requiring

The Greenhouse to stop providing services, or to notify data subjects of the breach, delete certain personal data held or prohibit certain types of processing.

Procedure

All staff must review the UK GDPR policies and procedures and guidance that are communicated to them.

The Greenhouse will nominate a person to be the Data Protection Officer/Privacy Officer. This is currently Head of Centre and Matt Cody.

The Greenhouse should ensure all staff understand the policies and procedures provided, including how to deal with a subject access request and what to do if a member of staff breaches UK GDPR.

The Greenhouse will consider providing training internally about UK GDPR (in particular, the Key Principles of UK GDPR) to all staff members.

The Greenhouse will delete any personal data that The Greenhouse no longer needs, based on the results of the audit conducted, taking into account any relevant guidance, such as the Records Management Code of Practice - see link in the Further Reading section.

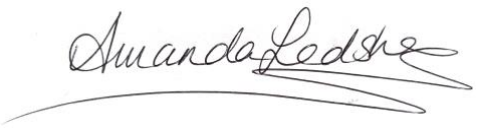
The Greenhouse will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with UK GDPR.

The Greenhouse will ensure it has privacy policies in place and will circulate them to data subjects as relevant.

The Greenhouse will ensure that, where required, proper consent to the UK GDPR standard is obtained from each Learner. The Greenhouse understands that the Consent Form provided may be used for this purpose.

The Greenhouse will ensure that processes and procedures are in place to respond to requests made by data subjects (including subject access requests) and to deal appropriately with any personal data breaches.

The Greenhouse will maintain a log of decisions taken and incidents that occur in respect of the personal data processed by The Greenhouse using the Data Protection Impact Assessment template at The Greenhouse.



Checked and reviewed: 21/07/2025

Next review due: 21/07/2026