GREENHEART
LEARNING PARTNERSHIP

DATA PROTECTION POLICY

Signed off by Trust Board: March 2026

Effective from: March 2026

Review Date: March 2027

Contents

1. Aims 2
2. Legislation and guidance 2
3. Definitions 3
4. The data controller 4
5. Roles and responsibilities 5
6. Data protection principles 6
7. Collecting personal data 6
8. Sharing personal data 9
9. Your rights 12
10. Parental requests to see the educational record 14
11. Biometric recognition systems 15
12. CCTV 15
13. Photographs and videos 15
14. Data protection by design and default 16
15. Data security and storage of records 19
16. Disposal of records 21
17. Personal data breaches 21
18. Training 22
19. Monitoring arrangements 22
20. Links with other policies 22

Appendix 1 - Personal Data Breach Procedure 23

Appendix 2 – Personal Data Security Breach Report 25

1. Aims

Greenheart Learning Partnership aims to ensure that all personal data collected about staff, pupils, parents / carers, Members, Trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- The Electronic Commerce (EC Directive) Regulations 2002
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- DfE (2024) 'Keeping children safe in education'

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

TERM	DEFINITION
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Greenheart Learning Partnership (The Partnership) processes personal data relating to parents / carers, Members, Trustees, visitors and others, and therefore is a data controller.

The Partnership is registered with the ICO, as legally required.

The Partnership 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 DPA, and will provide comprehensive, clear and transparent privacy policies. This will also provide evidence that it is complying with UK GDPR and DPA.

The Partnership will be able to demonstrate how data is processed across the Partnership, and will ensure each individual academy within the Partnership is adhering to the same procedure and that this is being implemented and enforced in line with the wider trust policies.

Additional internal records of the school's processing activities will be maintained and kept up to date. 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 school 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

5. Roles and responsibilities

This policy applies to all staff employed by the Partnership, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Partnership Board

The Partnership Board of Trustees has overall responsibility for ensuring that the Partnership and it's academies comply with all relevant data protection obligations.

Data protection officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the Partnerships compliance with data protection law, and developing related policies and guidelines, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.

The DPO will provide a termly report of activities directly to the Partnership Board and, where relevant, report to the board their advice and recommendations on Academy data protection issues.

Our DPO is Rhiannon Terry, Director of Corporate Affairs and Governance.

GLPDPO@greenheartlearning.org

The Partnerships DPO works centrally and in conjunction with) and Headteachers, who arethe nominated Data Protection Lead (DPL) at each of the academies. These leads are in place to support the management of data protection on a day-to-day basis.

For details of the data protection lead at each of the Partnerships academies please visit the Partnerships Website.

Headteacher/Executive Headteacher

The headteacher fulfils the role of the data protection lead and acts as the representative of the data controller on a day-to-day basis at the academies. In the instance where there are Executive Headteachers across multiple schools, the role of DPL will be overseen by the

Executive Headteacher and supported by the Head of School / Principal or Deputy Headteacher.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Partnership of any changes to their personal data, such as a change of address
- Contacting the DPO or Data Protection Lead in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that the partnership must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Partnership aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the partnership/academy can fulfil a contract with the individual, or the individual has asked the partnership/academy to take specific steps before entering into a contract
- The data needs to be processed so that the partnership/academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the partnership/academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the partnership/academy (where the processing is not for any tasks the partnership/academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

Privacy Notices

Privacy notices will be clear, transparent and accessible to identify how we process personal data for different stakeholders, including:

- The school workforce
- pupils
- volunteers
- parents/carers
- Trustees/Members
- Third parties and visitors.

These are available on the Partnership website and updated on a regular basis, or when a change in the processing activities takes place.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Partnership's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent when no other legal basis applies

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any people covered under this policy.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Automated decision making and profiling

The Partnership 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 child nor use special category personal data, unless:

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

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

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

Generative AI systems will not be used to make solely automated decisions with significant effects on individuals, such as decisions regarding academic grading, behaviour sanctions, admissions, or staff appraisals, unless a suitably qualified person reviews and authorises the decision-making outcome.

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 Partnership 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 Partnership 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.

10. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the Partnership's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency, and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

DPIAs will allow the Partnership to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Partnership'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 Partnership 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 Partnership will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

11. Record of Processing Activities

All organisations who process data should ensure that they have a ROPA, or 'Record of Processing Activity', which outlines:

- the organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
- the purposes of the processing;
- a description of the categories of individuals and of personal data;
- the categories of recipients of personal data;

- details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
- retention schedules; and
- a description of the technical and organisational security measures in place.

Documenting processing activities in this way is not only a legal requirement, but also makes it far easier to understand the data being held. Each Academy is responsible for managing their ROPA, with support from the DPO. A central ROPA is managed and updated by the Middle Leadership Team, supported by the DPO.

12. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Partnership holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the 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
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO at GLPDPO@greenheartlearning.org

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Partnership may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

You have the right to withdraw consent at any time by contacting the Headteacher of your school

To make a Subject Access Request for your personal information, or be given access to your child's educational record, contact the Headteacher of your school.

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with the school in the first instance via the Headteacher.

You can also contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or any individualWould reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably redact, and we don't have the other person's consent and it would be unreasonable to proceed without it

- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPL or DPO. If staff receive such a request, they must immediately forward it to the DPL, who will coordinate with the DPO for the Partnership.

13. Parental requests to see the educational record

There is no automatic parental right of access to the educational record for pupils in academies.

To make a Subject Access Request for your personal information, or be given access to your child's educational record, contact the Headteacher of your school who will advise further.

14. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any initial or future biometric recognition system is put in place or before their child first takes part in it. The Academy collecting this data will get written consent from at least one parent or carer before any biometric data is taken from their child and first process it.

Parents/carers and pupils have the right to choose not to use the Academy's biometric system(s). Alternative means of accessing the relevant services for those pupils will be provided, alternative arrangements will be on an academy by academy basis.

Parents/carers and pupils can withdraw consent, at any time, any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the data will not be processed irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the Academy's biometric system(s), consent will also be obtained before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Academy will delete any relevant data already captured.

15. CCTV

CCTV is used in various locations around the partnership sites to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

Individuals' permission is not required to use CCTV, but it is made clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Academy directly. Further guidance in relation to use of CCTV across the Partnership is available in the CCTV Policy.

16. Photographs and videos

As part of the Partnership's activities, we may take photographs and record images of individuals within the academies or at Partnership events..

Written consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at Academy/Partnership events for their own personal use are not covered by data protection legislation. However, it will be asked that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the Academy/Partnership takes photographs and videos, uses may include:

- Within Academy/Partnership on notice boards and in Academy/Partnershipmagazines, brochures, newsletters, etc.
- Outside of Academy by external agencies such as the school photographer, newspapers, campaigns
- Online on our Partnership/Academy website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted, where possible, and not distributed further.

When using photographs and videos in this way the partnership will not accompany them with any other personal information about the child, to ensure they cannot be identified, unless explicit consent has been granted for this Please see our Child Protection Policy for more information about how we use photographs and images.

17. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and CoPilot. Greenheart Learning Partnership recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Partnership will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

18. 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 Partnership 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. When assessing any cloud-based or AI-powered service, the school will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows the Partnership to audit or verify compliance where necessary. The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system is 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. This is done through the IT ticketing system and is managed centrally. Access for employees will be removed when they leave the Partnership and the IT will be informed through the offboarding process.

All files and personal data will be encrypted before they leave a school 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 Partnership devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the Partnership should unauthorised access, deletion or modification occur, using user libraries and access management, which will be reviewed on an annual basis or more regularly if required. This will ensure ongoing compliance with Partnership's policies for the use of cloud computing.

The Partnership's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the Head of IT. They 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.

With support from the DPO, the Head of IT 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 Partnerships 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 Partnership 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 Partnership is prepared to accept that risk.
- Monitor the use of the Partnerships cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the Executive Leadership Team.

19. Data Protection by design and default

Measures will be put in place to show that the Partnership has integrated data protection into all data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the Partnership's/Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters and keeping a record of completion/attendance
- Regularly conducting reviews and audits to test our privacy measures to ensure compliance
- Appropriate safeguards being put in place if personal data is transferred outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Partnership DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that is held, maintaining an internal record of the type of data, type of data subject, how and why the data is being used, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

20. Data security and storage of records

The Partnership aims to protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the Academy/Partnership office.
- Where possible, multi-factor authentication (MFA) or single sign on (SSO) through Microsoft Office365 is used for system access. Where this is not possible, the Partnership follows the National Cyber Security Centre advice regarding password policy, which recommends:
    - Using a password manager to securely store passwords.
    - Creating strong and memorable passwords using three random words.
    - Avoiding using predictable passwords such as dates, family and pet names.
    - Avoiding using the most common passwords that criminals can easily guess.
    - Not re-use the same password across important accounts.
    - Not automatically expiring passwords.
    - Only asking users to change their passwords on indication or suspicion of compromise.
    - Using delegation tools instead of password sharing.
-
- Encryption software is used to protect all portable devices and removable media, such as laptops
- USB devices and other removable storage devices are not permitted.
- Digital data is coded, encrypted or password-protected, on a clous based network that is regularly backed up.
- Where possible, the Partnership enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff, pupils, Members, Trustees and committee members who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our [Online-safety policy/ICT policy/Acceptable use agreement
- Where personal data is shared with a third party, carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see Section 8)

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 via MCAS or if sent through Outlook, they are 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

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of an academy or central office containing sensitive information are supervised at all times.

21. Safeguarding

Greenheart Learning Partnership understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The Partnership 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 pupils. The Executive Team 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 pupil in a timely manner.

The academy SLT will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child 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 SLT 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 child at risk. The academy will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

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

22. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the Partnership cannot or does not need to rectify or update it.

For example, paper-based records will be shredded or incinerated and electronic files overwritten or deleted. Third parties may be used to safely dispose of records on the Partnership's behalf. If this is done, the Partnership will require the third party to provide sufficient guarantees that it complies with data protection law.

23. Personal data breaches

The Partnership will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the partnership will follow the procedure set out in appendix 1.

When appropriate, the data breach will be reported to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.

- The theft of an Academy laptop containing non-encrypted personal data about pupils.

Once a member of staff identifies that there has been a data breach, they will complete the Brach Notification Form in appendix 2.

24. Training

All staff, Members, Trustees and committee members are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy's processes make it necessary.

25. Monitoring arrangements

The Data Protection Officer is responsible for monitoring and reviewing this policy with the support of the DPL and Executive Leadership Team

This policy will be reviewed annually and approved by Greenheart Learning Partnership Board of Trustees.

26. Links with other policies

This data protection policy is to be read in conjunction with any other relevant Partnership policies:

- Child Protection and Safeguarding
- Privacy Notices
- CCTV
- Online Safety
- ICT Policy
- Acceptable Use Agreement
- Records Management Policy
- Cyber Security
- Freedom of Information Policy
- Freedom of Information Publication Scheme

Appendix 1 - Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, Trusee or data processor must immediately notify the Headteacher who is the Data Protection Lead. The DPL will may need to inform the data protection officer (DPO). This should be done by completing the Breach Notification Form (Appendix 2)
- The Data Protection Lead (DPL) will investigate the report and determine whether a breach has occurred. To decide, the DPL will consider with support from the Partnership's DPO where necessary, whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Everyone covered under this policy will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPL will need to alert the DPO.
- The DPL will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help with this where necessary.
- The DPL will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPL will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool and DPL will alert the DPO who will liaise with the ICO.
- Where the ICO must be notified, the DPO will do this on behalf of the academy/Partnership.
- The DPO will report as much as they can within 72 hours of the Academy's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the Academy is required to communicate with individuals whose personal data has been breached, support and guidance will be provided by the DPO. This support and guidance will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The Data Protection Lead, supported by the DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Academy or Partnership will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the Academy's/Partnership IT system.

- The DPL and relevant parties will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPL will assess recorded data breaches and identify any trends or patterns requiring action by the Academies to reduce risks of future breaches

Actions to minimise the impact of data breaches

The below the steps have been set out to identify how to mitigate the impact of different types of data breaches if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and amendedas necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender, the and the DPL as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT departmentto attempt to recall it from external recipients and remove it from the Academy's email system (retaining a copy if required as evidence).

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPL must be informed and will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPL will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPL will carry out an internet search to check that the information has not been made public; if it has, the publisher/website owner or administrator will be contacted to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPL will inform the DSL and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's cashless payment provider being hacked and parents' financial details stolen.
- Hardcopy reports sent to the wrong pupils or families

Privacy Notices:
Alumni
Job Applicants
Member, Trustees, Committee Members and other Volunteers
Parents and Carers – Use of your Child's Personal Data
Parents and Carers – Use of your Personal Data
Partnership Workforce
Pupils' Own Data
Suppliers of Goods and Services
Visitors

Appendix 2 – Personal Data Breach Notification

Breach overview		
Date and time breach happened		
Data and time breach discovered		
Date and time informed the DPO		
Name of Staff reporting the breach		
Was the breach caused by you	Yes	No
If no – who caused the breach		
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, pupils, 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?	

Appenix 3 – Personal Data Breach Report

Time and Date breach was identified	
Academy	
Description of the Breach	
Name of Person Reporting it:	
Confirmed or suspected Breach	
Volume of Data Involved	
Breach contained or ongoing	
What actions were undertaken to recover the Data	
Any other relevant information	

A. Investigation Checklist A. Containment and Recovery

Determine severity of breach and if any Personal Data is involved	
Allocate Lead Investigation Officer	
Identify cause of the breach and whether it has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible	
Determine whether anything can be done to recover any losses and limit any damage that may be caused E.g. physical recovery of data / equipment, or where data corrupted, through use of back-ups.	

Where appropriate, the Lead Responsible Officer or nominee to inform the police. E.g. stolen property, fraudulent activity, offence under Computer Misuse Act	

B. Assessment of Risks

Type and volume of data How many individuals' Personal Data are affected by breach?	
How sensitive is the data?	
What happened to it?	
If the data was lost / stolen, were there any protections in place to prevent access / misuse? E.g. Encryption of data / device.	

Who are the individuals whose data has been compromised (students, applicants, staff, customers, clients or suppliers)? Is there actual / potential harm that could come to any individuals? E.g. Are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft / fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?	
Are there others who might advise on risks / courses of action? E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.	

C. Consideration of Further Notification

Can notification help the Partnership meet its security obligations under the seventh data protection principle? E.g. prevent any unauthorised access, use or damage to the information or loss of it.	
Can notification help the individual?	

D. Evaluation and Response

Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?	
Consider the dangers of 'over notifying'. Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work"	
Consult the ICO guidance on when and how to notify it about breaches. Where there is little risk that individuals would suffer significant detriment, there is no need to report. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of Personal Data. Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals. E.g. police, insurers, professional bodies, funders, trade unions, website / system owners, bank / credit card companies.	
Establish where any present or future risks lie.	
Consider and identify any weak points in existing security measures and procedures. E.g. in relation to methods of storage and / or transmission, use of storage devices, levels of access, systems/network protections.	
Consider and identify any weak points in levels of security awareness/training.	

Report to ELTand Partnership Trust Board	

Report Form Completed by: _____

Signature: _____

Date: _____