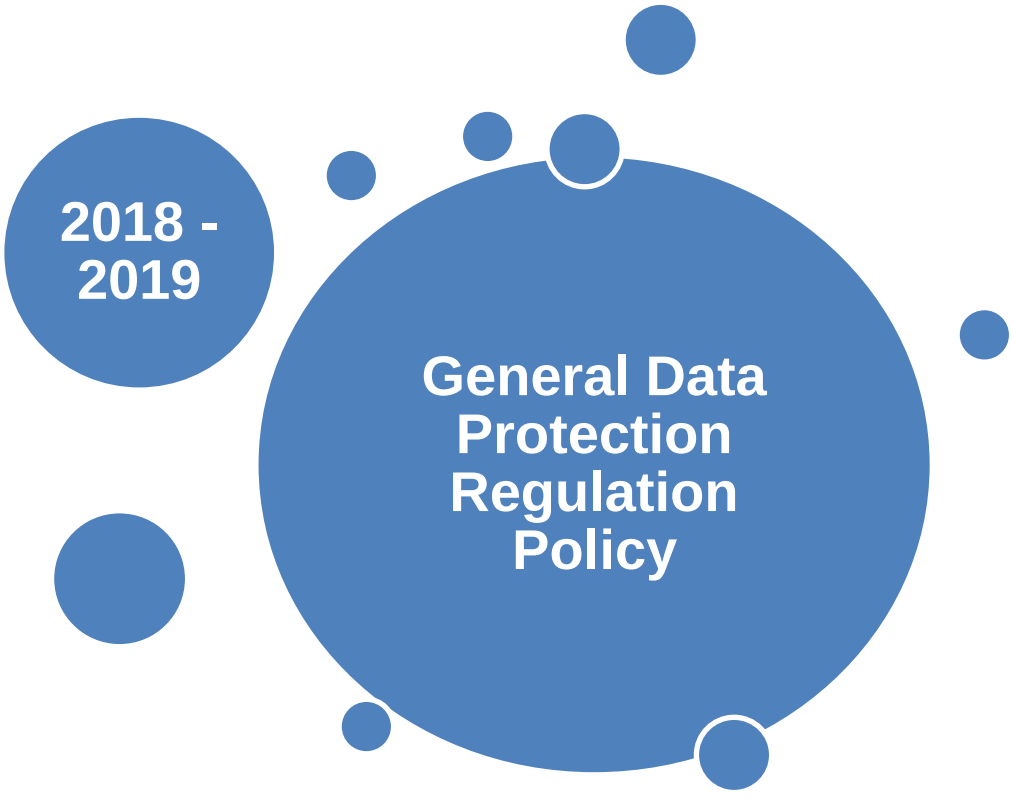
The ContinU Plus Academy

(Inclusive of WHP Service)



The ContinU Plus Academy

General Data Protection Regulation Policy

Contents

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

1. Aims

ContinU Plus Academy (hereafter CPA and inclusive of the WHP Early Intervention Family Support Service) aims to ensure that all personal data pertaining to staff, students, parents, governors, visitors and other individuals across the Trust is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill, as well as any other new legislation that may be introduced.

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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 code of practice 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, 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.
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

The CPA processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

CPA is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

The Trust has delegated responsibility to the headteacher, Sara Devo, for ensuring compliance with the GDPR and this policy within the day-to-day activities of the academy.

5. Roles and responsibilities

This policy applies to **all staff** employed by the CPA, and to external organisations or individuals working on the CPA's behalf. Staff members who fail to comply with this policy may face disciplinary action.

5.1 Governing Board

The CPA Governing Board has overall responsibility for ensuring that the CPA complies with all relevant data protection obligations.

5.2 Headteacher

The headteacher acts as a representative of the data controller on a day-to-day basis.

5.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the CPA processes, and for the ICO.

Our DPO is Lucy Hines and is contactable via lh555@cpa.worcs.sch.uk or telephone 01562 822463.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the CPA of any changes to their personal data, such as a change of address
- Contacting DPO 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 European Economic Area;
  - 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 GDPR is based on data protection principles that the CPA 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 CPA aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of the following 6 legal reasons to do so under GDPR law:

- The data needs to be processed so that the CPA can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the CPA can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the CPA, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the CPA 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 student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and expected provisions of the Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

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

7.2 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.

When staff members no longer require the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the CPA's Data Retention Schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so 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 as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the CPA 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 the criteria used to determine this period;
- The source of the data, if not directly from the individual;
- Whether any automated decision-making is being applied to their data (decisions taken with no human involvement, that might negatively affect them), and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing. In the case of the WHP Service these should be made to the Primary School that the child attends, who will then liaise with the WHP Service Manager.

If staff members receive a subject access request they must immediately forward it to the DPO, no information can be released without authorisation.

9.2 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 aged 12 and above are generally 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 students aged 12 and above may not be granted without the express permission of the student. Subject access requests from parents or carers of students below the age of 12 may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- Will require the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made by them;
- Will respond without delay and within 1 month of receipt of the request;
- Will provide the information requested 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 will not disclose information if:

- It could cause serious harm to the physical or mental health of the student or another individual;
- The disclosure of the information would not be in the child's best interests as it would reveal that the child is at risk of abuse;
- It contains adoption or parental order records;
- It is given to a court in proceedings concerning the child.

Repetitive requests for the same information or for further copies of the data will be deemed to be unfounded or excessive and the CPA reserves the right to charge a reasonable fee which takes into account administrative costs.

If the CPA has to refuse a subject access request, we will explain our reasoning to the individual, and inform them they have the right to complain to the ICO if they deem our reasons to be unjust.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request, and be informed when we are collecting data about how we use and process it, individuals also have the right to:

- Withdraw their consent at any time;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which the CPA has justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances);
- Object to decisions based solely on automated decision making or profiling;
- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO.

Individuals should submit any request to exercise these rights to the DPO. If staff members receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Under GDPR, parents/carers of students at the CPA do not have an automatic right to access their child's educational record. The CPA will respond to such requests in accordance with other Subject Access Requests as outlined in this policy.

11. CCTV

We use CCTV in various locations around the academy sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12. Photographs and videos

Photographs used for curricular, assessment, security, registration, training and development or travel reasons are essential for performing the public task of the CPA. They will not be used for any other purpose and will be deleted once a student is no longer in that setting or, at the point they are no longer needed for the specific purpose pertaining to the public task for which they are held.

As part of our day-to-day activities, we may take photographs and record images of individuals at the CPA. Uses may include:

- On school notice boards and in academy prospectus, newsletters, etc.;
- External agencies such as local newspapers or campaigns;

- Online on our website or social media pages.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Consent can be refused or withdrawn at any time. Should a parent/carer/student wish to withdraw their consent, we will delete the photograph or video and not distribute it further.

See our Safeguarding Children Policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our 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;
- Completing privacy impact assessments where the CPA'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, this and any related policies, ensuring compliance and any other data protection matters. Attendance records to all training sessions will be kept;
- Conducting termly reviews and audits to test our privacy measures and make sure we are compliant;
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the 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 we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will 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, pinned to notice/display boards, or left unattended anywhere else where there is general access at any time;
- Staff are provided with their own secure login and password to computer systems and these must not be shared with other users;
- Computer passwords must be at least 8 characters long containing letters and numbers. Staff are reminded to change their passwords at regular intervals;
- Encryption software will be used to protect all portable devices and removable media, such as laptops and USB devices;
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient;
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for academy-owned equipment (see our Acceptable Use Policy);
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected;
- Where personal information is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security. The person taking the information from the academy premises accepts full responsibility for the security of the data and ensuring they store it in a method that complies with this policy.

15. 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 we cannot or do not need to rectify or update it.

16. Personal data breaches

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

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

When appropriate, we will report the data breach to the ICO within 72 hours. Breaches which require reporting may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person;
- The theft of an academy laptop containing non-encrypted personal data about students;
- A non-anonymised dataset being published on the website which shows the exam results of students eligible for the pupil premium;
- Use of personal device to access personal data that is not securely password protected.

17. Training

All staff and governors will be 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 CPA's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if any changes are made to the GDPR that will affect the CPA's practice. Otherwise, or from then on, this policy will be reviewed annually and be ratified by the CPA Governing Board.

19. Links with other policies and documentation

This data protection policy is linked to other CPA policies as appropriate, examples below:

- Privacy Notice
- Freedom of Information Policy
- Staff Code of Conduct
- Safeguarding Children Policy
- Acceptable Use Policy
- Data Retention Schedule

Date Policy Created: **May 2018**

Member of Staff Responsible: Lucy Hines (School Business Manager)

Ratified by Governing Body: …… Date: …….

Review Date: **May 2019**

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
2. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    a. Lost;
    b. Stolen;
    c. Destroyed;
    d. Altered;
    e. Disclosed or made available where it should not have been;
    f. Made available to unauthorised people.
3. The DPO will alert the headteacher in the first instance.
4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. The DPO will advise on whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    a. Loss of control over their data;
    b. Discrimination;
    c. Identify theft or fraud;
    d. Financial loss;
    e. Unauthorised reversal of pseudonymisation (for example, key-coding);
    f. Damage to reputation;
    g. Loss of confidentiality;
    h. Any other significant economic or social disadvantage to the individual(s) concerned;
    i. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
7. The DPO will document the decision, in case it is challenged at a later date by the ICO or an individual affected by the breach.
8. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    a. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    b. The name and contact details of the DPO
    c. A description of the likely consequences of the personal data breach
    d. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

9. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. 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
10. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    a. The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. 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
11. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a. Facts and cause
    b. Effects
    c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    d. Records of all breaches will be kept in accordance with regulation.
13. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches
We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. Full guidance is given to staff as part of their induction to the Academy and initial training has been delivered to all current staff members.

Examples of relevant actions to be taken to mitigate the impact of a data breach involving risky or sensitive personal data:

Sensitive information being disclosed via email that is not password protected

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender of the email must attempt to recall the email as soon as they become aware of the error
- If the sender cannot recall the email for any reason, the DPO will contact the ICT department and ask them to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals, 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. A written response from all unauthorized individuals confirming they have complied with the request is required.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website immediately and all copies are deleted
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they are aware

A laptop containing non-encrypted sensitive personal data being stolen or hacked

- ICT department to remotely wipe data from the laptop
- Establish the facts – including exactly what information was held
- Communicate the breach to the data subjects without delay
- Notify relevant third parties that can help to mitigate the risk e.g. Police