



Dacorum Education
Support Centre

Data Protection Policy

1. POLICY STATEMENT AND OBJECTIVES

The objectives of this Data Protection Policy are to ensure that Dacorum Education Support Centre (the "Centre") and its Management Committee and employees are informed about, and comply with, their obligations under the General Data Protection Regulation (GDPR) and other Data Protection legislation.

The Centre is a maintained education support centre and is the Data Controller for all the Personal Data processed by the centre.

Everyone has rights regarding how their personal information is handled. During the course of our activities, we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, learners, parents / carers and other members of learners' families, management committee members, external providers, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in GDPR and other legislation. GDPR imposes restrictions on how we may use that information.

This policy does not form part of any employee's contract of employment, and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of GDPR may expose the centre to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the centre's employees. At the very least, a breach of GDPR could damage our reputation and have serious consequences for the Centre and for our stakeholders.

2. STATUS OF THE POLICY

This policy has been approved by the Centre's Management Committee. It sets out our rules on Data Protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3. DEFINITION OF TERMS

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

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

Data Controllers means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Data Users include employees, volunteers, and members of the Management Committee whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our Data Protection and security policies at all times;

Data Processors means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

DPIA means a Data Protection Information Audit

Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

Personal Data means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with GDPR;

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Sensitive Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, Biometric Data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation.

Data protection principles

Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data is accurate, having regard to the purposes for which they are processed and are erased or rectified without delay;
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals; and

- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. PROCESSED LAWFULLY, FAIRLY AND IN A TRANSPARENT MANNER

GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the centre), who the Data Controller's representative is (in this case the DPO), the purpose for which the Data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

- where we have the Consent of the Data Subject;
- where it is necessary for compliance with a legal obligation;
- where processing is necessary to protect the vital interests of the Data Subject or another person;
- where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

Sensitive Personal Data

The Centre will be processing Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Sensitive Personal Data.

When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

- the Data Subject's explicit consent to the processing of such Data has been obtained
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to Data Protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

The Centre recognises that in addition to Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be

implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

Criminal convictions and offences

There are separate safeguards in GDPR for Personal Data relating to criminal convictions and offences.

It is likely that the Centre will Process Data about criminal convictions or offences. This may be due to pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

In addition, from time to time we may acquire information about criminal convictions or offences involving learners or parents. This information is not routinely collected and is only likely to be processed by the Centre in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the Data secure.

Transparency

One of the key requirements of GDPR relates to transparency. This means that the Centre must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The centre has developed privacy notices for the following categories of people:

- learners
- parents
- staff
- Management Committee

The Centre wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to centre premises or if we ask people to complete forms requiring them to provide their Personal Data.

We will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a learner; and free of charge.

Consent

The Centre must only process Personal Data based on one or more of the lawful bases set out in GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than consent.

A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

If we are relying on consent as a basis for Processing Personal Data about learners, if a learner is aged under 13, we will need to obtain consent from the Parent(s). If we require Consent for Processing Personal Data about learners aged 13 or over, we will require the consent of the learner although, depending on the circumstances, the Centre should consider whether it is appropriate to inform Parents about this process. Consent is likely to be required if, for example, the Centre wishes to use a photo of a learner on its website or on social media. Consent is also required before any learners are signed up to online learning platforms. Such consent must be from the parent if the learner is aged under 13. When relying on consent, we will make sure that the learner understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented. Unless we can rely on another legal basis of processing, explicit consent is usually required for Processing Sensitive Personal Data. Often, we will be relying on another legal basis (and not require explicit consent) to process most types of Sensitive Data.

Evidence and records of consent must be maintained so that the Centre can demonstrate compliance with consent requirements.

5. DATA PROTECTION OFFICER

The Data Protection Officer (the “DPO”) is responsible for ensuring the Centre is compliant with GDPR and with this policy. This post is held by Stephen Peach, Business Manager, (dpo@desc.herts.sch.uk). Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

The DPO will play a major role in embedding essential aspects of GDPR into the Centre’s culture, from ensuring the Data Protection principles are respected to preserving Data Subject rights, recording Data Processing activities and ensuring the security of processing.

The DPO should be involved, in a timely manner, in all issues relating to the protection of Personal Data. To do this, GDPR requires that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

- senior management support
- time for DPOs to fulfil their duties
- adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate
- official communication of the designation of the DPO to make known existence and function within the organisation
- access to other services, such as HR, IT and security, who should provide support to the DPO;
- continuous training so that DPOs can stay up to date with regard to Data Protection developments
- where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member

- whether the Centre should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

The DPO is responsible for ensuring that the centre's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the Centre must ensure the independence of the DPO.

The Centre will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the Management Committee.

The requirement that the DPO reports directly to the Management Committee ensures that the Centre's Management Committee members are made aware of the pertinent Data Protection issues. If the Centre decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Management Committee and to any other decision makers.

A DPO appointed internally by the Centre is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with his or her role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.

To avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing Personal Data. Senior management positions are likely to cause conflicts. Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

In the light of this and if the centre decides to appoint an internal DPO, the Centre will take the following action in order to avoid conflicts of interests:

- identify the positions incompatible with the function of DPO
- draw up internal rules to this effect to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate.
- include a more general explanation of conflicts of interests
- declare that the DPO has no conflict of interests with regard to his or her function as a DPO, as a way of raising awareness of this requirement
- include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest

If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO.

6. SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject.

The Centre will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that

disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

Adequate, relevant and limited to what is necessary

The Centre will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

In order to ensure compliance with this principle, the Centre will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a business function and we should not collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

The Centre will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis.

When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the Centre's Data Retention guidelines.

7. ACCURATE AND, WHERE NECESSARY, KEPT UP TO DATE

Personal Data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed. If a Data Subject informs the Centre of a change of circumstances their records will be updated as soon as is practicable.

Where a Data Subject challenges the accuracy of their data, the Centre will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

A Data Subject continues to have rights under GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedures set out in this document have been followed.

Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed

Personal Data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete data is properly erased. The Centre has a retention schedule for all data.

8. DATA TO BE PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY OF THE PERSONAL DATA

The Centre has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Anonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must follow all these procedures and technologies and must comply with all applicable aspects of our Data Security Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with GDPR and relevant standards to protect Personal Data.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the Data can access it
- **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed
- **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes

It is the responsibility of all members of staff and members of the Management Committee to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher or the DPO.

Please see our Data Security Policy for details for the arrangements in place to keep Personal Data secure.

Management Committee Members

Members of our Management Committee are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, learner exclusions or parent complaints. Management Committee members should be trained on the Centre's Data Protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

- Ensure that Personal Data which comes into their possession as a result of their Centre duties is kept secure from third parties, including family members and friends
- Ensure they are provided with a copy of the Centre's Data Security Policy
- Using a DESC email account for any centre-related communications

- Ensuring that any centre-related communications or information stored or saved on an electronic device or computer is password protected and encrypted
- Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be accessed by third parties

Members of our Management Committee will be asked to read and sign an Acceptable Use Agreement.

9. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw consent to processing at any time
- receive certain information about the Data Controller's Processing activities
- request access to their Personal Data that we hold
- prevent our use of their Personal Data for direct marketing purposes
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- restrict processing in specific circumstances
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- request a copy of an agreement under which Personal Data is transferred outside of the EEA
- object to decisions based solely on Automated Processing, including profiling (Automated Decision Making)
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms
- make a complaint to the supervisory authority (the ICO); and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format

We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

10. DEALING WITH SUBJECT ACCESS REQUESTS

GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The Centre can invite a Data Subject to complete a form, but we may not insist that they do so.

It is important that all members of staff can recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the Centre from responding to the request as being made under GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 **working** days.

Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is **one working month**.

It should be noted that the time for responding to a request stops during periods when the Centre is closed for the holidays. Should the situation arise, we will attempt to mitigate any impact this may have on the rights of Data Subjects to request access to their Data by implementing the following measures:

- encourage Data Subjects to avoid sending requests during periods when the centre is closed
- The DPO's email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur
- ensure the dpo@desc.herts.sch.uk email address can be accessed by more than one member of staff and will be monitored regularly
- The DPO will have the contact details for the following:
 - Headteacher
 - IT support
 - legal advisors and our insurers
- The DPO to report any notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the Centre is closed and has limited staff available due to holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the Centre should take to mitigate any risks
- ensure GDPR is an agenda item at Management Committee Meetings
- regular meetings with a team of staff concerning GDPR issues

A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the DPA 1998).

The Centre will ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

To ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

Requests from learners who are considered mature enough to understand their rights under GDPR will be processed as a Subject Access Request as outlined below and the data will be given directly to the learner (subject to any exemptions that apply under GDPR or other legislation). As the age when a young person is deemed to be able to give consent for online services is 13, we will use this age as a guide for when learners may be considered mature enough to exercise their own Subject Access Rights. In every case it will be for the Centre, as Data Controller, to assess whether the child can understand their rights under GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

Requests from learners who do not appear to understand the nature of the request will be referred to their parents or carers.

Requests from parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the learner is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the Centre considers the child to be mature enough to understand their rights under GDPR, the Centre shall ask the learner for their consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the parent (subject to any enactment or guidance which permits the Centre to disclose the Personal Data to a parent without the child's consent). If consent is not given to disclosure, the Centre shall not disclose the Personal Data if to do so would breach any of the Data Protection principles.

It should be noted that the Education (Pupil Information) (England) Regulations 2005 applies to maintained schools so the rights available to parents in those regulations to access their child's educational records apply to the Centre. This means that following receipt of a request from a parent for a copy of their child's educational records, the centre must provide a copy within **15 Centre working days** (excluding holidays), subject to any exemptions or court orders which may apply. The Centre may charge a fee for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a Subject Access Request.

Following receipt of a Subject Access Request, and provided that there is sufficient information to process the request, an entry should be made in the centre's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of data required (e.g. Learner Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Where requests are "manifestly unfounded or excessive", because they are repetitive, the Centre can:

- charge a reasonable fee considering the administrative costs of providing the information; or
- refuse to respond

Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.

You may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

In the context of a school a Subject Access Request is normally part of a broader complaint or concern from a parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is considered when responding to a request and seek advice if required on managing the broader issue and the response to the request.

PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the centre whilst also applying common sense to the circumstances. They should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked
- Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information

AUTHORISED DISCLOSURES

The Centre will only disclose data about individuals if one of the lawful bases apply.

Only authorised and trained staff are allowed to make external disclosures of Personal Data. The Centre will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Local Authorities
- the Department for Education
- the Disclosure and Barring Service
- the Teaching Regulation Agency
- the Teachers' Pension Service
- the Local Government Pension Scheme
- Herts for Learning
- Serco
- HMRC
- the Police or other law enforcement agencies
- our legal advisors and other consultants
- insurance providers
- occupational health advisors
- exam boards including AQA, Pearsons.
- External Providers including C&G Plastering, XC Centre, Building One Zone, Aspire
- YC Hertfordshire
- the Joint Council for Qualifications.
- NHS health professionals including educational psychologists and school nurses.
- Attendance Improvement Officer
- Courts, if ordered to do so
- Prevent teams in accordance with the Prevent Duty on schools
- other schools, for example, if we are negotiating a managed move and we have consent to share information in these circumstances
- confidential waste collection companies
- staff insurance & well-being providers including Schools Advisory Service

Some of the organisations we share personal data with may also be Data Controllers, in which case we will be joint controllers of personal data and may be jointly liable in the event of any data breaches.

Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is processed ("GDPR clauses"). A summary of GDPR requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the Centre to ensure that GDPR clauses have been added to the contract with the Data Processor. Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

In some cases, Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with GDPR, including responsibility for any Personal Data Breaches, onto the Centre. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

11. REPORTING A PERSONAL DATA BREACH

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (for example sending an email or SMS to the wrong recipient)
- Unforeseen circumstances such as a fire or flood
- Hacking, phishing and other “blagging” attacks where information is obtained by deceiving whoever holds it

When does a personal data breach need to be reported?

DESC must notify the Information Commissioners Office of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect include:

- potential or actual discrimination
- potential or actual financial loss
- potential or actual loss of confidentiality
- risk to physical safety or reputation
- exposure to identity theft (for example through the release of non-public identifiers such as passport details)
- the exposure of the private aspect of a person’s life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

12. REPORTING A DATA BREACH

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Complete a Data Breach Report Form (Appendix 1)
- Email the completed form to the Business Manager
- Notify the Headteacher that a data breach has taken place

Breach reporting is encouraged throughout DESC and staff are expected to seek advice from the HR Manager (Jill Clark) or Business Manager (Stephen Peach) if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals.

Once reported, you should not take any further action in relation to the breach. You must not notify any affected individuals or regulators or investigate further. The Business Manager will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report.

Managing and recording the breach

On being notified of a suspected personal data breach, the Business Manager will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to:

- Where possible, contain the data breach
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- Assess and record the breach in the centre's data breach register
- Notify the Information Commissioner's Office
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breach.

Notifying the ICO

The Business Manager will notify the Information Commissioner's Office when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and within 72 hours of becoming aware of the breach. If the centre is unsure of whether to report a breach, the assumption will be to report it.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Business Manager will notify the affected individuals without undue delay including the name and contact details of the Information Commissioner's Office, the likely consequences of the data breach and the measures the Centre have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Business Manager will co-operate with and seek guidance from the Information Commissioner's Office and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Centre will consider alternative means to make those affected aware (for example by making a statement on the centre website).

Notifying other authorities

The centre will need to consider whether other parties need to be notified of the breach. For example:

- Insurers
- Parents
- Third parties (for example when they are also affected by the breach)
- The Local Authority
- The police (for example if the breach involved theft of equipment or data) This list is non-exhaustive.

13. ASSESSING THE BREACH

Once initial reporting procedures have been carried out, the centre will carry out all necessary investigations into the breach.

The Centre will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the Centre will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the Information Commissioner's Office and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is
- The volume of data affected
- Who is affected by the breach (i.e. the categories and number of people involved)
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise
- Are there any protections in place to secure the data (for example, encryption, password protection)?
- What has happened to the data
- What could the data tell a third party about the data subject
- What are the likely consequences of the personal data breach on the centre
- Any other wider consequences which may be applicable

14. PREVENTING FUTURE BREACHES

Once the data breach has been dealt with, the Centre will consider its security processes with the aim of preventing further breaches. To do this, we will:

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether it is necessary to conduct a privacy or data protection impact assessment
- Consider whether further audits or data protection steps need to be taken
- Update the data breach register
- Debrief the Management Committee following the investigation
- Any trends identified from data breaches each term will be discussed at termly Management Committee Meetings.

Reporting data protection concerns

Prevention is always better than dealing with data protection as an afterthought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the Business Manager. This can help capture risks as they emerge, protect the Centre from data breaches and keep our processes up to date and effective.

Monitoring

This policy will be monitored by the Management Committee who will receive updates regarding data breaches from the Business Manager and the Headteacher.

Related policies

Staff should refer to the following policies that are related to this Data Protection policy: -

- E-Safety, ICT and ICT Security policy
- Data Protection and Data Breach policy
- Freedom of Information Policy
- Safeguarding Policy
- Staff Code of Conduct Policy

These policies are also designed to protect Personal Data and can be found on the Centre website.

15. ACCOUNTABILITY

The Centre must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with Data Protection principles. The Centre is responsible for, and must be able to demonstrate, compliance with the Data Protection principles.

The Centre must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive team accountable for Data Privacy
- implementing Privacy by Design when processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where processing presents a high risk to rights and freedoms of Data Subjects
- integrating Data Protection into internal documents including this Data Protection Policy, related policies and Privacy Notices
- regularly training employees and Management Committee members on GDPR, this Data Protection Policy, related policies and Data Protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The Centre must maintain a record of training attendance by centre personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort

16. RECORD KEEPING

GDPR requires us to keep full and accurate records of all our Data Processing activities.

We must keep and maintain accurate records reflecting our processing including records of Data Subjects' Consents and procedures for obtaining consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

17. TRAINING AND AUDIT

We are required to ensure all centre personnel have undergone adequate training to enable us to comply with Data Privacy laws. We must also regularly test our systems and processes to assess compliance.

Members of staff must attend all mandatory Data Privacy related training.

18. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like anonymisation) in an effective manner, to ensure compliance with Data Privacy principles.

This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by considering the following:

- the state of the art
- the cost of implementation
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing

We are also required to conduct DPIAs in respect to high risk processing. The Centre should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (applications, systems or processes), or changing technologies (applications, systems or processes);

We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to learners. If our processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

A DPIA must include:

- a description of the processing, its purposes and the Centre's legitimate interests if appropriate
- an assessment of the necessity and proportionality of the processing in relation to its purpose
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

19. CCTV

The Centre uses CCTV in locations around the site. This is to:

- protect the buildings and their assets
- increase personal safety and reduce the fear of crime
- support the Police in a bid to deter and detect crime
- assist in identifying, apprehending and prosecuting offenders
- provide evidence for the Centre to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, learners or other visitors on the site which breaches or is alleged to breach the centre's policies
- protect members of the centre community, public and private property; and
- assist in managing the Centre

Please refer to the centre's CCTV policy/code of practice for more information.

20. POLICY REVIEW

It is the responsibility of the Management Committee to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

This policy should be reviewed by the centre periodically and at least every 2 years. It is important to ensure that the DPO is aware of their obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

21. ENQUIRIES

Further information about the centre's Data Protection Policy is available from the DPO. General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

22. Appendix 1 – GDPR Clauses

GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))
2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))
3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)
4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))
5. The Processor must ensure it flows down GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))
6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3)(e))
7. The Processor must assist the Data Controller with their security and Data Breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))
8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))
9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3)(g))
10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))
11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3))



Dacorum Education
Support Centre

Data Protection Policy – Confirmation of Receipt

I _____ acknowledge that on
_____ (date) I received a copy of DESC Data Protection Policy and that I
have read and understood it.

Signature: _____

Name: _____

23. APPENDIX 3: DATA BREACH REPORTING FORM

| Summary of Incident | |
|--|--|
| Date and time of incident | |
| Number of people whose data is affected | |
| Nature of breach, e.g. theft/disclosed in error/technical problems | |
| Description of how breach occurred | |
| Reporting | |
| When was the breach reported? | |
| How did you become aware of the breach? | |
| Who has been informed? ICO/LA etc. | |
| Personal data | |
| Full details of personal data involved (without identifiers) | |
| Number of individuals affected | |
| Have all affected individuals been informed? | |
| If not, why not? | |
| Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so please give details. | |

| Data retrieval | |
|--|--|
| What immediate remedial action was taken? | |
| Has the data been retrieved or deleted? If yes date and time | |
| Impact | |
| Describe the risk of harm to the individual as a result of this incident. | |
| Describe the risk of identity fraud as a result of this incident | |
| Have you received a formal complaint from any individual affected by this breach? If so give details | |
| Management | |
| Do you consider that the employee(s) involved has breached information governance policies and procedures? | |
| Please inform of any disciplinary action taken in relation to the employee(s) involved | |
| Had the employee(s) completed data protection training? | |
| As a result of this incident do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so what steps have been taken to address this? | |
| Has there been any media coverage of the incident? If so please provide details | |

| | |
|--|--|
| <p>What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure</p> | |
|--|--|

Name

Signature

Date
