LORDSWOOD GIRLS' SCHOOL & SIXTH FORM CENTRE

This policy is called:	Data Protection Policy
It applies to:	Lordswood Girls' School & Sixth Form Centre
Person responsible for its revision:	Headteacher
Status:	Statutory
Website?	School website and staff launch page
Approval by:	Governing Body
Review frequency:	Must be reviewed at least every two years
Date of last review:	June 2020
Date of next review:	June 2022

Statement of intent

Lordswood Girls' School & Sixth Form Centre is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the General Data Protection Regulation 2016.

The GDPR and this policy apply to all of Lordswood Academies Trust personal data processing functions, including those performed on pupils', clients', employees', volunteers', suppliers' and partners' personal data, and any other personal data the Trust and its school process from any source.

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially social services.

The Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to the Trust's activities. This register needs to be available on the supervisory authority's request.

This policy applies to all governors, employees and volunteers of Lordswood Academies Trust and any other interested parties, such as outsourced suppliers of services. Any breach of the GDPR will be dealt with under the disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for Lordswood Academies Trust and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Trust without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Lordswood Academies Trust is committed, and which gives the Trust the right to audit compliance with the agreement.

This policy is in place to ensure all staff and governors are aware of their responsibilities under the General Data Protection Regulation and outlines how the Trust complies with the following core principles of the Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.
- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to the data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

1. Data Controller

Lordswood Academies Trust, as the corporate body, is the data controller.

1.1 Governors and all those in managerial or supervisory roles throughout the Trust are responsible for developing and encouraging good information handling practices.

1.2 The Data Protection Officer, a role specified in the GDPR, is accountable to the Governing Body and Senior Management Team of Lordswood Girls' School & Sixth Form Centre for the management of personal data within the school and Trust and for ensuring that compliance with data protection legislation and good practice can be demonstrated. The Data Protection Officer for the Trust is the Director of Finance. The accountability of the Data protection Officer includes:

1.2.1 development and implementation of the GDPR as required by this policy; and

1.2.2 security and risk management in relation to compliance with the policy.

1.3 The Data Protection Officer has direct responsibility for ensuring that Lordswood Academies Trust complies with the GDPR, as do all staff in respect of data processing that takes place within their area of responsibility.

1.4 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for employees seeking clarification on any aspect of data protection compliance.

1.5 Compliance with data protection legislation is the responsibility of all governors, employees and volunteers of the Trust who process personal data.

1.6 All governors, staff and volunteers are required to have undertaken data protection awareness training, the nature of which will be decided by the frequency of processing and the nature of the personal data they may process.

1.7 Governors, employees and volunteers are responsible for ensuring that any personal data about them and supplied by them is accurate and up-to-date.

1.8 The Trustees of the Trust have overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

1.9 On occasion, personal information may be processed by the Trust's HR providers, Mazars Payroll Services and the Department for Education. By involving another organisation in the data processing, the Trust signs up to an increase in certain risks, for instance, fraud. The security of the personal information is covered in a written agreement/formal contract between the Trust and the relevant organisation.

2. Guidelines for staff

- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records should not be left unattended or in clear view anywhere with general access.
- Computerised data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device must be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks should not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices must be password-protected to protect the information on the device in case of theft.
- Where possible, the Trust enables electronic devices to allow the remote blocking/deletion of data in case of theft.
- Staff and governors are not permitted to use their personal laptops or computers for school purposes.
- All necessary staff are provided with their own secure login and password.
- Emails containing sensitive or confidential information should be password-protected if there are insecure servers between the sender and the recipient.
- Circular emails to parents should be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff must check that the recipient is correct before sending.
- The Trust uses encryption software to protect all electronic devices, and ensures encryption settings are always up-to-date. Staff have been issued with encrypted flash drives for when external work is required.
- Personal information that could be considered private or confidential should not be taken off the school premises, either in electronic or paper format. Where this is unavoidable, staff must take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises must accept full responsibility for the security of the data.
- Before sharing data, all staff must 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 the school containing sensitive information must be supervised at all times.
- The Trust will not publish any personal information, including photos, in newsletters, on its website or other media without the consent of the data subject.

- When uploading information to the school website, staff must be considerate of any metadata or deletions which could be accessed in documents and images on the site.
- The Trust is aware that CCTV recording of images of identifiable individuals constitutes processing personal information, so must be done in line with data protection principles.
- The Trust notifies all students, staff and visitors of the purpose for collecting CCTV images via notices.
- Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose, i.e. the security and the safety of staff and students.
- The school keeps CCTV footage for one month for security purposes. The Director of Finance is responsible for keeping the records secure and allowing access.
- The school will always indicate its intentions for taking photographs of students and obtain permission before publishing them.
- If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent/guardian of the pupil.
- Precautions will be taken when publishing photographs ofstudents, in print, video or on the website.
- Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the General Data Protection Regulation.

3. Data protection principles

3.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. This policy is designed to ensure compliance with the principles.

3.2 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources. The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The Trust's Privacy Notice Procedure will ensure that the information provided to the data subject includes as a minimum:

3.2.1 the identity and the contact details of the controller and, if any, of the controller's representative;

3.2.2 the contact details of the Data Protection Officer;

3.2.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

3.2.4 the period for which the personal data will be stored;

3.2.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

3.2.6 the categories of personal data concerned;

3.2.7 the recipients or categories of recipients of the personal data, where applicable;

3.2.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

3.2.9 any further information necessary to guarantee fair processing.

3.3 Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner's Office (ICO) as part of Lordswood Academies Trust GDPR register of processing.

3.4 Personal data must be adequate, relevant and limited to what is necessary for processing

3.4.1 The Data Protection Officer is responsible for ensuring that Lordswood Academies Trust and its school do not collect information that is not strictly necessary for the purpose for which it is obtained.

3.4.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

3.4.3 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by to ensure that collected data continues to be adequate, relevant and not excessive.

3.5 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

3.5.1 Data that is stored by the School and Trust must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

3.5.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

3.5.3 It is also the responsibility of students/their parents and employees/volunteers (the data subject) to ensure that data held by the school and Trust is accurate and up-to-date. Completion of an information checking form will include a statement that the data contained therein is accurate at the date of submission.

3.5.4 Governors, employees, volunteers, and students/their parents are required to notify the School/Trust of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Lordswood Academies Trust and its school to ensure that any notification regarding change of circumstances is recorded and acted upon.

3.5.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

3.5.6 The Data Protection Officer will review annually the retention dates of all the personal data processed by Lordswood Academies Trust by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted or destroyed.

3.5.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If Lordswood Academies Trust decides not to comply with the

request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the ICO and seek judicial remedy.

3.5.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned.

3.5.9 The Data Protection Officer is also responsible for passing any correction to the personal data to the third party where this is required.

3.6 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

3.6.1 Where personal data is retained beyond the processing date, it will be minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.

3.6.2 Personal data will be retained in line with the current Records Retention Schedule, and, once its retention date is passed, it will be securely deleted or destroyed.

3.6.3 The Data Protection Officer must specifically approve any data retention that exceeds the defined retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

3.7 Personal data must be processed in a manner that ensures the appropriate security

The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of Lordswood Academies Trust's controlling or processing operations.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or students) if a security breach occurs, the effect of any security breach on the Trust itself, and any likely reputational damage including the possible loss of trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate and relevant national or international security standards.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout the school and Trust;
- The inclusion of data protection in employment contracts;
- Possible disciplinary action measures for data breaches;
- Physical access controls to electronic and paper based records;

- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

3.8 <u>The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)</u>

The accountability principle in Article 5(2) of the GDPR requires Data Controllers to demonstrate that they comply with the principles and states explicitly that this is their responsibility. Lordswood Academies Trust will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as completing and updating data protection impact assessments (DPIAs), breach notification procedures and incident response plans.

4. Data subjects' rights

4.1 Data subjects have the following rights in relation to data processing, and the data that is recorded about them:

4.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

4.1.2 To prevent processing likely to cause damage or distress.

4.1.3 To prevent processing for purposes of direct marketing.

4.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

4.1.5 To not have significant decisions that will affect them taken solely by automated process.

4.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

4.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

4.1.8 To make a request to the ICO to assess whether any provision of the GDPR has been contravened.

4.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

4.1.10 To object to any automated profiling that is occurring without consent.

4.2 Lordswood Academies Trust ensures that data subjects may exercise these rights:

4.2.1 Data subjects may make data access requests as described in the Trust's Subject Access Request Procedure; this procedure also describes how the Trust will ensure that its response to the data access request complies with the requirements of the GDPR.

4.2.2 Data subjects have the right to complain to Lordswood Academies Trust in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line the Trust's standard Complaints Procedure.

5. Consent

5.1 'Consent' is taken to mean that the data subject has explicitly given their agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

5.2 'Consent' also means that the data subject has been fully informed of the intended processing and has signified their agreement on the basis of the information provided; NB consent obtained on the basis of misleading information will not be a valid basis for processing.

5.3 Consent must be actively obtained; consent cannot be inferred from a non-response to a communication.

5.4 The Trust and its school must be able to demonstrate that consent was obtained for the processing operation.

5.5 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

5.6 In most instances, consent to process personal and sensitive data is obtained routinely by Lordswood Academies Trust and its school using standard consent documents or statements on forms.

5.7 Where online services are provided to students, parental or guardian authorisation must be obtained. This requirement applies to children under the age of 16.

6. Security of data

6.1 All governors, employees and volunteers are responsible for ensuring that any personal data that the school and Trust hold and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the school/Trust to receive that information and has entered into a confidentiality agreement.

6.2 All personal data should be accessible only to those who need to use it, and all personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected; and/or
- stored on computer media which are encrypted.

6.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised personnel. All governors, employees and volunteers are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.

6.4 Manual records must not be left where they can be accessed by unauthorised personnel nor removed from school premises without explicit authorisation. As soon as manual records are no longer required for day-to-day business use, they must be removed to secure archiving or securely destroyed.

6.5 Personal data may only be deleted or disposed of in line with the Records Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

7. Disclosure of data

7.1 Lordswood Academies Trust will ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All governors, employees and volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Trust's business.

7.2 The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:
to safeguard national security;
prevention or detection of crime including the apprehension or prosecution of offenders;
assessment or collection of tax duty;
discharge of regulatory functions (includes health, safety and welfare of persons at work);
to prevent serious harm to a third party; and
to protect the vital interests of the individual in life and death situations.

7.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

8. Retention and disposal of data

8.1 Lordswood Academies Trust and its school will not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

8.2 The data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

8.3 The retention period for each category of personal data will be set out in the Records Retention Procedure along with the criteria used to determine this period including any statutory obligations Lordswood Academies Trust has to retain the data.

8.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done securely.

9. Information asset register/data inventory

9.1 Lordswood Academies Trust has established a Personal Data Inventory as part of its approach to addressing risks, thus determining:

- business processes that use personal data;
- sources of personal data;
- description of each item of personal data;
- processing activity;
- who maintains the inventory of data categories of personal data processed;
- who documents the purpose(s) each category of personal data is used for;
- recipients and potential recipients of the personal data;
- all retention and disposal requirements.

9.2 Lordswood Academies Trust is aware of any risks associated with the processing of particular types of personal data.

9.2.1 The Trust assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by the Trust and in relation to processing undertaken by other organisations on behalf of the Trust.

9.2.2 Lordswood Academies Trust will manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

9.2.3 Where a type of processing, in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, the Trust will, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data.

9.2.4 Appropriate controls will be applied to reduce the level of risk associated with processing individual data to an acceptable level and the requirements of the GDPR.

10. Monitoring

The Data Protection Officer is responsible for the day to day implementation of this policy. The Governing Body will monitor implementation of the policy through the KRA link governor.

11. Review

This policy will be reviewed by the Trust every two years, or more frequently if required.

Links to other policies

- Freedom of information
- Publication scheme
- Confidentiality
- ICT
- E-safety
- Social Media
- Mobile phone

ANNEX 1

1. Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC, including the UK's 1998 Data Protection Act. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge and, wherever possible, that it is processed with their consent.

a. Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) **–** the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

b. Article 4 definitions

Establishment **–** the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – 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.

Special categories of personal data – 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 natural person's sex life or sexual orientation.

Data controller – 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – 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.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.