WATFORD COMMUNITY SPORTS & EDUCATION TRUST
REGISTERED CHARITY NO: 1102239

Data Protection Policy

Introduction

The 2018 Data Protection Act (DPA 2018), came into force on 23 May 2018 and together with the General Data Protection Regulation (2016) (GDPR), establishes the legal framework for the handling of personal data for individuals within the EU and applies to UK individuals.

The principles and procedures set out in this policy must be followed at all times by the Watford FC Community Sports and Education Trust (the Trust), it's staff, volunteers, agents, contractors and other parties working on behalf of the Trust. These principles and procedures apply to personal information processed by the Trust on behalf of, or in regard to employees, clients, participants, trustees, volunteers, agents and contractors.

The Trust's Community Director has overall responsibility for data protection within the Trust but each individual who is processing data is acting on the Trust's behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

Processing of information – how information is used, stored and managed.
Information Commissioner (ICO) - formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Controller – used to denote the entity which determines the purposes and means of processing personal data.
Processor – A processor is responsible for processing personal data on behalf of a controller.
Personal data – any information which enables a person to be identified
Special categories of personal data –These are considered to be more sensitive and may only be processed in more limited circumstances.

1.The Data Protection Principles

Watford FC's Community Sports and Education Trust is required to comply with the principles of good information handling, the GDPR and the Data Protection Act 2018 and to follow the principles set out in the GDPR.

These principles require the Trust to ensure that all personal data must be**:**

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. 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, historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the GDPR in order to safeguard the rights and freedoms of the data subject.
6. 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.

2. The Lawful Basis for processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies (Article 6 GDPR)

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3. What do we need to tell people?

The Trust will include information about the lawful basis (or bases, if more than one applies) in our privacy notices. Under the transparency provisions of the GDPR, the information we need to give people includes:

- our intended purposes for processing the personal data; and
- the lawful basis for the processing.

This applies whether we collect the personal data directly from the individual or collect their data from another source.

4.Privacy Notices

Any process which gathers personal and/or special categories of personal data will adopt a privacy notice to be given to the data subject. The privacy notice will contain the following information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice
- What to do if they want to complain to or about us

A fuller Privacy Policy will also be published on our website.

5. What about special category data?

When processing special category data, we will identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9 of the GDPR. We shall document both our lawful basis for processing and our special category condition so that we can demonstrate compliance and accountability.

6. Individual Rights

Individuals have specific rights in relation to the information we hold about them, they have the right to;

- know how we use their personal information
- access their personal information
- have personal information corrected if it is inaccurate or incomplete
- ask us to delete personal information when we no longer need it
- ask us to restrict how we process their information
- get their information from us and re-use it across other services
- object to certain ways we use their information
- be safeguarded against risks where decisions based on their information are taken entirely automatically
- tell us if we can share their information with 3rd parties
- tell us their preferred frequency, content and format of our communications with them

Please refer to Annex 1 for more details about each of these rights and how we manage them.

Individuals can exercise these rights by contacting our Data Protection Officer (contact details below).

7.What information do we collect and why?

The Trust collects and processes the personal data set out in Part 14 of this Policy. This includes:

- Personal data collected directly from data subjects; and
- Personal data obtained from third parties.
- The Trust only collects, processes, and holds personal data for the specific purposes set

out in Part 14 of this Policy (or for other purposes expressly permitted by the GDPR).
- Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Annex 1 for more information on keeping data subjects informed.

8.Adequate, Relevant, and Limited Data Processing

The Trust will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Parts 3 and 4, above, and as set out in Part 14, below.

9. Accuracy of Data and Keeping Data Up-to-Date

The Trust shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Annex 1.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

10. How long do we keep information?

The Trust shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

The Trust's approach to data retention is;

- For data of any participant or supporter of the Trust, the Trust will hold their data for no longer than 6 years from that person's last contact with the Trust. This corresponds with the maximum length of time within which a claim can be brought against the Trust.
- For employees of the Trust, their data will be held for no longer than 7 years after termination of their contract. This corresponds with the maximum length of time within which an investigation can be initiated by HMRC.
- For recruitment data, this will be held for no longer than 1 year after the recruitment process has ended, unless the candidate withdraws their consent.

11. Secure Processing

The Trust shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 15 to 21 of this Policy.

12. Accountability and Record-Keeping

The Trust's Data Protection Officer is Steve Alexander, dpotrust@watfordfc.com.

The Data Protection Officer shall be responsible for overseeing the implementation of this policy

and for monitoring compliance with this policy, the Trust's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

The Trust shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Trust, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Trust collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Trust, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Trust; and
- Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

13. Data Protection Impact Assessments

The Trust shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Trust's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Trust; and
- Proposed measures to minimise and handle identified risks

14. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Trust;

Details of the Type and Purpose of Data held can be found within the Trust's Personal Data Information Asset Register. If you would like to see a copy of the register then please contact the Trust's Data Protection Officer at dpotrust@watfordfc.com

15. Data Security - Transferring Personal Data and Communications

The Trust shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be password protected;
- All emails containing personal data must be marked "confidential";

- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient;
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media should be treated as confidential and always transported securely. Where appropriate, this data should be stored in a folder or container marked "confidential".

16. Data Security – Storage

The Trust shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords, both to access the electronic device, and to access the document containing the personal data.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically is backed up daily via onsite servers;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Trust or otherwise without the formal written approval of your line manager and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Trust where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Trust that all suitable technical and organisational measures have been taken).
- personal information must not be left unattended and/or in clear view during the working day

17. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to section 10.

Disposal of any personal data in hardcopy must be shredded or put into secure data sacks for shredding by a GDPR compliant organisation.

18. Data Security - Use of Personal Data

The Trust shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, volunteer, agent, sub-contractor, or other party working on behalf of the Trust requires access to

any personal data that they do not already have access to, such access should be formally requested from your line manager in the first instance, and in instances where significant quantities of data or sensitive personal data are requested, also from the Data Protection Officer.

- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- Where personal data held by the Trust is used for marketing purposes, it shall be the responsibility of the individual employee who is sending out the marketing correspondence, to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

19. Data Security - IT Security

The Trust shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Trust is designed to require such passwords.;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Trust, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Trust's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Trust-owned computer or device without the prior approval of your senior manager in the first instance and then relevant IT supplier.

20. Organisational Measures

The Trust shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Trust shall be made fully aware of both their individual responsibilities and the Trust's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, volunteers, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust;
- All employees, volunteers, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so;
- All employees, volunteers, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised;
- All employees, volunteers, agents, contractors, or other parties working on behalf

of the Trust handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Trust shall be reviewed periodically, as set out in section 9;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Trust arising out of this Policy and the GDPR; and
- Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

21. Transferring Personal Data to a Country Outside the EEA

The Trust may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

22. Data Breach Notification

All personal data breaches must be reported immediately to the Trust's Data Protection Officer and handled in accordance with the Trust's Data Breach process. All breaches shall be recorded in the Trust's Personal Data Incident and Breach log.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Trust's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

23.If someone wants to contact us or complain to us

To exercise any individual rights, request information about our privacy policy, know more about the information we hold or make a complaint about how we've handled personal information, data subjects can email us at dpo@ofgem.gov.uk or write to:

The Data Protection Officer
Watford FC CSE Trust
Vicarage Road Stadium
Vicarage Road
Watford
WD18 0ER

24. Complaints to the Information Commissioner

Data subjects have a right to complain to the Information Commissioner

If they want to complain about how we have handled their information they can report it direct to the Information Commissioner's Office at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire

SK9 5AF
Telephone: 0303 123 1113
Online: Live chat

25. Implementation of Policy

This Policy shall be deemed effective as of 21st May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Policy Name	Data Protection and Privacy Policy
Effective Date	Oct-2018
Next Review Date	Jun-20
Drafted By:	Compliance, Risk and Data Protection Manager
Approved by Board	Oct-2018

Annex 1

Individual Rights

1.**Keeping Data Subjects Informed**

The Trust shall provide the information to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

- Details of the Trust including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 14 of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 21 of this Policy for further details);
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to the Trust's processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

2. **Data Subject Access**

- Data subjects may make subject access requests ("SARs") at any time to find

out more about the personal data which the Trust holds about them, what it is doing with that personal data, and why.

- Employees who receive a SAR should use a Receipt of Subject Access Request Form, sending the form to the Trust's interim Data Protection Officer at dpotrust@watfordfc.com within 24 hours of receiving the request.
- Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the Trust's Data Protection Officer.
- The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.
- The Trust will respond to an SAR using one of the following electronic formats: Pdf, docx, xlsx, xlsm.
- Data subjects who make an SAR are required to provide two forms of identification. These can incluce; Passport, Driving Licence, Birth Certificate, Bank Statement and Utility Bill (from last 3 months).

3. **Rectification of Personal Data**

- Data subjects have the right to require the Trust to rectify any of their personal data that is inaccurate or incomplete.
- The Trust shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Trust of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

4. **Erasure of Personal Data**

- Data subjects have the right to request that the Trust erases the personal data it holds about them in the following circumstances:
    - It is no longer necessary for the Trust to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
    - The data subject wishes to withdraw their consent to the Trust holding and processing their personal data;
    - The data subject objects to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so)
    - concerning the right to object);
    - The personal data has been processed unlawfully;
    - The personal data needs to be erased in order for the Trust to comply with particular legal obligation**;**

- The personal data is being held and processed for the purpose of providing information society services to a child.

- Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

5. **Restriction of Personal Data Processing**

- Data subjects may request that the Trust ceases processing the personal data it holds about them. If a data subject makes such a request, the Trust shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

6. **Data Portability**

- Where data subjects have given their consent to the Trust to process their personal data, or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
- To facilitate the right of data portability, the Trust shall make available all applicable personal data to data subjects in the following format:

  Email, and password protected
- Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
- All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

7. **Objections to Personal Data Processing**

- Data subjects have the right to object to the Trust processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for historical research and statistics purposes.
- Where a data subject objects to the Trust processing their personal data based on its legitimate interests, the Trust shall cease such processing immediately, unless it can be demonstrated that the Trust's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
- Where a data subject objects to the Trust processing their personal data for direct marketing purposes, the Trust shall cease such processing immediately.
- Where a data subject objects to the Trust processing their personal data for

historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

8. **Profiling**

- The Trust does not currently use personal data for profiling purposes.
- In the future when personal data is used for profiling purposes, the following shall apply:

  Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

  Appropriate mathematical or statistical procedures shall be used;

  Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

  All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 15 to 19 of this Policy for more details on data security).