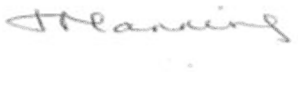
Data Protection GDPR Policy

Policy Ref: TMP40v2

This policy will not discriminate either directly or indirectly against any individual on grounds of sex, race, ethnicity or national origin, gender, sexual orientation, marital status, religion or belief, age, disability, socioeconomic status, offending background or any other personal characteristic.

Prepared By	Jackie Manning,	**Reviewed By**	Martin Heaton
Job Title	Assistant Director, Designated Safeguarding Lead	**Job Title**	Director
Signed		**Signed**	
Date	**July 2020**	**Date**	**July 2020**

Record of Changes

Version	Issue Date	Changes	Initials
v1	July 2019	Initial issue	JM
v2	July 2020	General procedural review, references updated, formatting changes	JM

Date of Next Review: July 2021

Scope

This Policy (and the other policies and documents referred to in it) sets out the basis on which TMP College will collect and use Personal Data either where TMP College collects it from individuals itself, or where it is provided to TMP College by third parties.

It also sets out rules on how TMP College handles, uses, transfers and stores Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

This policy should be read in conjunction with the following TMP College documents:

- TMP College Document Retention Policy
- TMP College Data Rights Policy
- TMP College Data Breach Policy
- TMP College Privacy Notice for Learners

A full list of definitions is provided in Appendix 1.

Overview

TMP College needs to collect, store and process personal data in order to carry out its functions and activities as a college. There are many reasons why we need to collect information including Safeguarding, for Health and Safety, to draw down funding for learners, to take fee payments or pay bursaries, or monitoring learning activity are just a few of these reasons. All staff members within TMP College are committed to protecting the confidentiality and integrity of the personal information it collects in line with the Data Protection Act 2018[1] and General Data Protection Regulation (GDPR) 2016[2].

Under data protection law we have to provide details of how our organisation handles personal data about staff, learners and customers for the data protection register.

As an organisation that collects, uses and stores personal data about its employees, learners, suppliers, partners, governors, parents and visitors, TMP College recognises that having controls around the collection, use, retention and destruction of personal data is important to comply with our obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR[3].

TMP College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of TMP College staff contract of employment and TMP College reserves the right to change this Policy at any time. All members of staff are obliged to comply with this Policy at all times.

[1] https://ico.org.uk/for-organisations/data-protection-act-2018/
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[3] https://gdpr-info.eu/art-5-gdpr/

TMP College's Personnel's General Obligations

All TMP College Personnel must comply with this policy.

TMP College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

TMP College Personnel must not release or disclose any Personal Data:

- outside TMP College; or
- inside TMP College to Personnel not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

TMP College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside TMP College.

Data Protection Principles

When using Personal Data, Data Protection Laws require that TMP College complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed; 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.

These principles are considered in more detail in the remainder of this Policy.

In addition to complying with the above requirements TMP College can demonstrate its accountability in adhering to data protection regulations through the other controls it has in place including, but not limited to, its Data Retention Policy, Data Breach Policy, Data Rights Policy, and its Privacy Notice for Learners.

TMP College also undertook a large scale scoping exercise and data protection audit before GDPR came into effect to ensure all information and processes were recorded, and processing scaled back to only include what was required. TMP College will continue to review and develop its compliance under GDPR and will complete in-year audits to monitor internal processes.

Lawful Use of Personal Data

TMP College lawfully processes Personal Data under the legal basis set out in Article 6[4] of the GDPR.

The majority of processing by TMP College is done because it is necessary for the performance of the tasks carried out in the Public Interest. We limit the information we collect to ensure we only collect what is needed to perform this duty effectively and without penalty.

TMP College also seeks to obtain the consent from individuals for the purpose of college activities, either where explicit consent is required (where it is specific, freely given and informed) or where we consider it important that the individual is made aware of the processing even if consent is not required.

Our Privacy Notice for Learners forms part of our new learner enrolment process and is designed to ensure all learners, staff and parents of children are fully informed of how their data will be used.

Every information asset containing Ordinary personal data held by TMP has been detailed in our Information Asset Register. This register details the lawful basis for the collection and processing of all the information we hold. For more information on the lawful basis used for processing please see https://ico.org.uk.

Additional conditions are imposed on TMP College where it uses Special Categories of Personal Data (as detailed in Article 9[5]). All Special Category data is also detailed in the Information Asset Register with confirmation of how these conditions are met. Additional information on Special Categories is given here[6].

TMP College also reserves the right to use other legal basis in its operational day to day activities where processing is necessary for legitimate interests, performance of a contract, compliance with legal obligations, or in order to protect the vital interests of individuals

If TMP College changes how it uses Personal Data, it will update this record and may also need to notify Individuals about the change. If TMP College Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

[4] https://gdpr-info.eu/art-6-gdpr/
[5] https://gdpr-info.eu/art-9-gdpr/
[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

Transparent Processing – Privacy Notices

TMP College endeavours to be as transparent about the processing of individual data as it can be, and demonstrates this with the Privacy Notices available to students in their enrolment, staff in their induction process, parents of children under 16 and suppliers.

Our Privacy Notices provide individuals with a summary of:

- the purpose for collecting the information;
- the safeguards we put in place to protect the data;
- individual's rights in relation to the data we collect;
- how long we retain the data for, and
- any third parties we share the information with.

Although we make reference to the generic retention of the information in our privacy notices, we have many sources of data and many sets of information that we hold so it is difficult to detail all of them in the notice specifically whilst trying to keep it accessible and retain simplicity.

TMP College's Information Asset Register details all of the retention and destruction periods as set out by the individual processing laws or by the senior managers that control the use of that data. Information on retention and destruction periods can be obtained from the Data Protection Officer.

If TMP College receives Personal Data about an Individual from other sources, TMP College will provide the Individual with a privacy notice about how TMP College will use their Personal Data. This will be provided as soon as reasonably possible.

If TMP College changes how it uses Personal Data then these privacy notices may be updated as required, but all individuals will be informed of any changes.

Whilst the majority of information provided to TMP College by individuals is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, TMP College will inform individuals whether they are required to provide certain information to us or if they have a choice in this.

How we use Personal Information in TMP College

We use Personal Information to manage individual's education, provide welfare and pastoral care, to track progress so we can help our learners achieve the best they can.

This may include every day activities such as creating class lists for tutrs at the start of the course, providing registers for tutors to mark attendance, registering with the awarding bodies to allow us to enter learners for exams, or providing a support plan or exam assessment.

For learners enrolling with TMP for post 14 qualifications, the Learning Records Service will give us a learners unique learner number (ULN) and may also give us details about previous learning or qualifications. We also use this information to improve and develop teaching and services in the future.

TMP College will only share personal data with third parties as part of the statutory duties placed on us or as declared in the Privacy Notice for Learners. We do not share information about our learners with anyone without consent unless the law and our policies allow us to do so.

As part of the public task placed on us by the Education and Skills Funding Agency (ESFA) to fund education we have a duty to provide them with eligibility, enrolment and achievement data for all our learners. This may be directly or indirectly as a sub-contractor of a prime provider.

Data is shared via our prime contractors for our 16-18 year olds with the Department for Education (DfE) on a similar statutory basis. This data sharing underpins school funding, educational attainment policy and monitoring. To find out more about the data collection requirements placed on educational institutions by the Department for Education see the links below.[7][8][9]

We may also share individual's personal information with local authorities and schools but only in relation to education, to provide appropriate support, or to transfer information to other educational institutions which learners may move to.

Young people have to remain in training or education until they are 18, so if a learner withdraws from our education programme before this age then we notify the Local Authority to highlight that the learner may have become 'Not in Education, Employment or Training' (NEET). As part of the same legal duty we may also provide destinations data to them. In both circumstances this will only be shared with the relevant local authorities on a need to know basis.

We may also pass student information to our Local Authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 16-19 year olds under section 507B of the Education Act 1996. However the parent / guardian of a 14-16 learner can request that only their child's name, address and date of birth is passed to their Local Authority or provider for the purposes of providing youth support services (once confirmed in writing to the 14-16 office). This right is transferred to the learner once he/she reaches age 16.

Personal Data must be kept up to date and relevant

TMP College is required to ensure that the Personal Data it holds is accurate and kept up to date.

TMP College has actively been taking steps to minimise the amount of information it collects and will continue to challenge internal processes to ensure data minimisation is at the forefront of our privacy by design development.

Enrolment forms and Learning Agreements for learners were updated for the 18/19 academic year to ensure we remove any personal information we do not need and learners can opt out of providing information that is not mandatory.

[7] https://www.gov.uk/guidance/complete-the-school-census
[8] https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information
9 https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

New processes and systems are currently being developed for the 20/21 academic year to ensure personal data can be kept up to date by individuals themselves and accuracy remains paramount. Internal audits take place to review the accuracy of the data we keep, and any corrections are made.

Data Protection Laws require that TMP College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a Privacy Notice and as set out in TMP College's record of how it uses Personal Data.

All TMP College Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected.

All TMP College Personnel that obtain Personal Data from sources outside TMP College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require TMP College Personnel to independently check the Personal Data obtained.

In order to maintain the quality of Personal Data, all TMP College Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not apply to Personal Data which TMP must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

TMP College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. TMP College has a Data Rights Policy which sets out how TMP responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with this document.

Personal Data must not be kept for longer than needed

Data Protection Laws require that TMP College does not keep Personal Data longer than is necessary for the purpose, or purposes, for which it was collected.

This Data Protection Policy should be read in conjunction with the TMP College Document Retention Policy which details the requirements and reasoning for TMP College retains information and how it is deleted or destroyed. This is linked to TMP Information Asset Register where the retention periods for all information is detailed specifically in relation to the purpose that piece of information was collected for, any legal all public task requirements, and the operational activity undertaken.

TMP College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by TMP, the reasons for those retention periods and how TMP securely deletes Personal Data at the end of those periods. These are set out in the TMP College Document Retention Policy.

If TMP College Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention and Destruction Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or TMP's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

Data Security

TMP College takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

TMP College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

Data Breach

TMP College has put a Data Breach Policy in place to both mitigate the risk of a breach occurring and to ensure there are appropriate procedures in place to respond. The objective of the Data Breach Policy is to enable staff to act promptly to contain any breaches that occur, minimising the risk associated with the breach and to take action if necessary to secure personal data and prevent further breaches.

TMP expects its staff to embed security and prevention practices in their normal working day to ensure personal, or special category, data is protected for the purposes of college business and must take appropriate steps to safeguard this information.

TMP College is undergoing GDPR training to ensure all staff are aware of the data protection regulations, and fully understand their role duties and responsibilities in protecting and safeguarding the personal data we collect. This is a key part of TMP College's security arrangements to help prevent a breach from occurring in the first place.

Additional IT security measures are also being implemented to protect TMP College networks and emails.

All TMP College Personnel have a duty to immediately report any breach to the Data Protection Officer. All breaches big or small, regardless of the harm or potential harm, should be identified and reported. Failure to follow the correct procedure or ignoring a possible data breach may result in disciplinary action.

Whilst TMP College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens College Personnel must comply with TMP College's Data Breach Policy.

A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

There are three main types of Personal Data breach which are as follows:

- Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and
- Integrity breach - where there is an unauthorised or accidental alteration of Personal Data.

Appointing Contractors who Access TMP College's Personal Data

TMP College may appoint contractors to work on our behalf to deliver aspects of college business that either TMP College is not best placed to deliver or is not suitably equipped to deliver. It may also utilise contractors for short term work, or where better economies of scale, breadth or expertise can be offered by a third party.

If TMP College appoints a contractor who is a Processor of TMP College's Personal Data, Data Protection Laws require that TMP College only appoints them where TMP College has carried out sufficient due diligence and only where TMP College has appropriate contracts in place.

A requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing contractors. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

A Processor is considered as having been appointed where TMP College engages someone to perform a service on our behalf and as part of it they may get access to our Personal Data. Where we appoint a Processor in this way TMP College, as Controller, remain responsible for what happens to the Personal Data.

Any contract where an organisation appoints a Processor must be in writing. GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

In addition the contract should set out:

- The subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller.

Individual's Rights

The GDPR legislation clearly details that individuals have the right to be informed about how we collect and process their personal information, but it goes deeper than that in giving them more control about how their data is collected, stored, and what is done with it once the processing is complete.

TMP College is fully aware of its legal obligations to allow individuals to exercise their rights over their Personal Data, and has therefore developed a specific Data Rights Policy to ensure that all individuals understand the process for applying their rights.

Marketing and Consent

Marketing consists of any advertising or marketing communication that is directed to particular individuals. TMP College uses a variety of marketing techniques to attract learners, employers and the public.

TMP College can contact Individuals to send them marketing or to promote itself, but where this is done it will only be done in a legally GDPR compliant manner where we have obtained consent.

TMP College provides more detail in their privacy notices, learning agreements and college signage to state where profiling takes place; and will require an individual's consent as a "clear affirmative action" to be contacted for marketing purposes.

TMP College is also aware of the Privacy and Electronic Communications Regulations 2003 (PECR)[10] that sit alongside data protection. The PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It also applies to any electronic communication which TMP College sends out including telephone calls, emails and text messages.

All electronic marketing communications from TMP College will ask individuals to opt in to the services they receive.

Alternatively, TMP College is able to market using a “soft opt in” if the following conditions are met:

- contact details have been obtained in the course of an enquiry;
- TMP College is marketing its own similar services; and
- TMP College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after.

Automated Decision Making and Profiling

Automated Decision Making would happen if TMP College made a decision about an Individual solely by automated means without any human involvement and the decision had legal or other significant effects. Profiling would happen if TMP College automatically used Personal Data to evaluate certain things about an Individual.

Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated decision making is very limited in TMP College, and nearly all processes have some human involvement at some point to ensure no individual is disadvantaged or treated unfairly.

There are some operational activities in TMP College where profiling occurs but any outcome or decision as a result of the profiling activity is ultimately made by human involvement.

TMP College undertakes ongoing monitoring of its operational activities where profiling or automated decision making may potentially occur.

Any Automated Decision Making or Profiling which TMP College carries out can only be done once TMP College is confident that it is complying with all applicable Data Protection Laws. If TMP College Personnel therefore wish to carry out any Automated Decision Making or Profiling, then they must inform the Data Protection Officer. College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

TMP College does not carry out Automated Decision Making or Profiling in relation to its employees.

[10] https://ico.org.uk/for-organisations/guide-to-pecr/

Data Protection Impact Assessments (DPIA)

TMP College actively promotes a Privacy by Design approach and ensures Data Protection Impact Assessments are undertaken when there is a change to a system, service or process.

The TMP College leadership and management team are responsible for any new IT projects, software or system implementation at TMP College. Part of the rigorous process for approving new IT projects now includes GDPR compliancy checks for any new supplier. This will include assessing whether the supplier has appropriate IT infrastructure and security measures in place, as well as assessing their GDPR compliance in relation to Policies and Procedures should a data breach occur. If the Supplier is appointed, then part of this process will also include setting up data sharing agreements, and assessing whether a DPIA is required before the project implementation starts.

If the DPIA is required for an IT Project or an internal process change then the GDPR legislation requires TMP College to put in place a number of steps to control any such changes to processing.

TMP College will carry out a risk assessment in relation to the use of Personal Data for a new service, product, process or project. This must be done prior to the processing via a Data Protection Impact Assessment (DPIA).

A DPIA should be started as early as practical in the design period of the project. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and the measures to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

All DPIAs must be reviewed and approved by the Data Protection Officer. Any privacy risks identified should either be mitigated for with an appropriate solution, or be monitored during the project and the DPIA revisited.

Appendix 1: Definitions

TMP College – TMP Studios CIC, 830 Ormskirk Road, Pemberton, Wigan, WN5 8EX

College Personnel – Any employee, worker or contractor who accesses any of TMP College's Personal Data and includes employees, consultants, contractors, subcontractors, agency staff or temporary staff hired to work on behalf of TMP College.

Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. TMP College acts as Controller in relation to areas such as the collection of employee details or enrolment information collected for its learners. It is the organisation itself which is the Controller not the staff.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – TMP College's Data Protection Officer is **Jackie Manning** and can be contacted via the main TMP College telephone number 01942 212607 or on email via jackiemanning@music-projects.com

EEA – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Individuals – Living individuals who can be identified, directly or indirectly, from information that TMP College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include our partners and employers.

Personal Data – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, health data, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

Processor – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. College examples include, software support we receive for our college student record system, which contains Personal Data, and outsourcing delivery of learning where we define the purpose and the processing requirements involved.

Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health (including learning difficulties or disabilities), sexual life or sexual orientation and criminal convictions. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.