Policy Name	Data Protection Policy
Approved by	FGB
Date of Approval	09/10/23
Date of Next Review	Autumn 24
Review Cycle	Annual
Type of Policy	Statutory
Data Protection Officer	Judicium
Policy Published on School Website	Yes
This Policy should be read in conjunction with	Data Breech Policy Data Retention Policy Cyber Security Policy

Data Protection Policy

Last Reviewed: September 2023
Next Review Date: September 2024

1. Purpose

1.1 This policy is intended to provide guidance to staff members so that personal and sensitive data is dealt with properly and securely and in accordance with the Data Protection Act of 1998 and in agreement with the key principles of the General Data Protection Regulation. This policy supplements the school's policy on data protection in order to provide further guidance and clarification to staff.

1.2 It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data or a need to have access to that data.

1.3 The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

2. Legislation

2.1 This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR, 2020) which was incorporated legislation adopted by the UK following the withdrawal from the European Union as well as the Data Protection Act (2018).

2.2 The policy is informed by guidance from the Information Commissioner's Office (ICO) and also reflects the ICO's guidance on the use of security surveillance cameras.

2.3 In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Key Principles of Data Protection

3.1 Data protection has a set of key principles that must be followed for the school to be compliant with data protection regulations.

3.1.1 Purpose Limitation

The school and its wider community must only collect, store or share data that is relevant to our purpose (in the context of running the school). These identified valid grounds for collecting and using personal data are known as our 'lawful basis'.

3.1.2 **Lawfulness, Fairness & Transparency**
The school must be clear, open and honest with people from the start about how it will use their personal data.

3.1.3 **Data Minimisation**
The school must be clear about what the personal data is being collected and used for from the start. All personal data must only be used for the purpose specified.

3.1.4 **Accuracy**
Collected data must be kept up-to-date. Reasonable steps must be taken to ensure the personal data held at the school is not incorrect or misleading as to any matter of fact.

3.1.5 **Storage Limitation**
Personal data must only be stored for a specified period. Individuals have a right to erasure if you no longer need the data.
There is currently no 'sector wide data retention policy' to guide schools but further guidance on how long data may be legally stored can be found on the GDPR School Toolkit Annex 5:1.

3.1.6 **Accountability**
Individuals must take responsibilities for how they store and use personal data lawfully, clearly and in a transparent manner. Compliance with data protection regulation is the responsibility of the whole school community not just the school as a data controller.

3.1.7 **Integrity & Confidentiality (Security)**
Data must be stored in a secure location. All staff members will ensure that appropriate security measures are in place to protect the personal data held.

4. Responsibilities

4.1 **All staff** employed by the school, and all external organisations or individuals working on our behalf, are responsible for storing and sharing data appropriately in accordance with the principles of data protection and the school's Data Protection Policy.

4.2 **All staff** must be responsible for reporting any actual or possible data breaches to the designated person.

4.3 **All staff** must be aware of their accountability if acting in contradiction to the school's Data Protection Policy. Failure to comply with this policy may result in disciplinary action.

4.4 The head teacher has overall responsibility for ensuring that staff are aware of the school's Data Protection policy and that adequate provisions have been made to support staff with this.

4.5 The governing body has overall responsibility for ensuring that the school is compliant with its relevant data protection obligations.

4.6 The school's data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and

guidelines where applicable. Our DPO is Craig Stilwell at Judicium Education (72 Cannon Street, London, EC4N 6AE) and is contactable by telephone (0203 326 9174) or email: dataservices@judicium.com.

5. Data Collected

5.1 Our school collects both sensitive and personal data so that it is able to carry out its official functions in the public interest as an institute for education (e.g. deliver education), or in order to meet a legal requirement (e.g. to ensure you meet health and safety requirements).

5.2 The Information Commissioners Office (ICO) classify data into personal data and sensitive data.

5.2.1 Personal data is information that relates to an identified or identifiable individual. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

- Names
- Addresses
- UPN
- Teacher assessments
- Free School Meal or Pupil Premium applicability
- Photographs/videos
- Contact details (phone numbers/emails)
- Date of birth

If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual *(i.e. If the school has a low percentage of pupils who are EAL, then this could be considered identifiable information)*.

Further guidance on whether data is identifiable can be found here.

5.2.2 Sensitive data is a special category of personal information that is identifiable to the individual, which, should it become public knowledge, have a detrimental effect on the individual *(i.e. for example, by putting them at risk of unlawful discrimination)*.

- Race
- Ethnic origin
- Political opinions
- Religious beliefs
- Medical information
- Safeguarding/child protection
- Sexual orientation
- Trade union membership
- Adoption or lac
- Visa application

Following best practice in DfE guidance, we also treat the following data as special category data:

- Safeguarding Matter
- Pupils in receipt of Pupil Premium
- Pupils with Special Educational Needs and Disability (SEND)
- Children in Need (CIN)
- Children Looked After by a Local Authority (CLA)

5.3 Information that is truly anonymous is not covered by the GDPR and therefore falls outside the regulations laid out in this policy.

5.4 The school must have a valid lawful basis in order to collect personal data (it must be necessary for the school to function). The school's privacy policy includes further information on the lawful basis in which the school collects personal data. If the school can reasonably achieve the same purpose without collecting the data, you will not have a lawful basis.

5.5 The school collects data from the pupils, staff members, parents, governors, volunteers and contractors who work at the school.

6. Processing & Sharing Data

6.1 All individuals who have access to data, including governors, volunteers and contracted professionals, will not share personal data with any third parties without consent, unless covered by the school's lawful basis.

6.2 For all processes not covered by lawful basis, consent must be sought from the individual or, in the case of the pupils, from the parent or carer. When asking for consent it is important to abide by the following guidelines:

- We use clear, plain language that is easy to understand.
- Be specific what the data is going to be used for and by whom.
- Keep a record of the consent

For some data processes, it may be easier to anonymise the data. As stated earlier, anonymised data falls outside data protection legislation as long as an individual is not identifiable.

6.3 If a member of staff wants to set up a new data process that involves the sharing of personal data, then they must consult the data protection team. Depending on the nature of the new process, the staff member may be referred to the school's DPO for further advice.

6.4 When considering setting up a new data process that involves sharing personal data that is of high risk, the school will complete a data protection impact assessment to help identify and minimise any potential risks. The school uses the ICO's Lawful basis interaction guidance tool to help ascertain whether the school has the legal right to process particular personal data and on what grounds to do so.

6.5 The school will still share data with the local authority and Department for Education if there is a legal obligation to do so.

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

6.7 Safeguarding

Safeguarding: data protection policies and procedures do **not** prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **Information can be shared without consent if to gain consent would place a child at risk.** Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place

6.8 Cyber Security

It's essential to ensure critical data is protected from cyber-attacks and unauthorised access. The school has detailed logs of the data stored within the school and what is stored outside of the school's direct control. Regular cyber security training supports all staff with safe and secure use of online technology at the school and the role they play in protecting the data we hold.

6.9 The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR.

7. Storing Data

7.1 All staff members must understand their role in managing and properly storing all personal data securely. Clear guidance on retention periods can be found in the school's Data Retention Policy.

7.2 Sensitive personal data, within the school, should be stored in a lockable drawer or cabinet where access is limited. Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access. This is unless it is under the school's lawful basis to educate or for health and safety reasons.

7.3 Staff are strongly discouraged to take paper records that contain personal data off of the school site. When staff do choose to take data off of the school site, they agree to take full accountability for keeping it secure and confidential until it is returned to the school site.

7.4 T**he school has a zero tolerance policy on using personal storage devices or any other personal technology to store personal or sensitive school related data**. This includes USBs and external harddrives. Data must only be stored on school owned devices and in accordance with the principles of data protection stated above. Failure to comply could result in disciplinary actions should a data breach occur.

7.5 All staff with laptops have had them encrypted to reduce the possibility of data being easily attainable should they be lost or accessed by another.

7.6 Personal data that is no longer needed or is no longer covered by the school's lawful basis, will be securely disposed of. This covers but physical data and that stored digitally.

7.7 School governors will also have an oversight role in making sure their school has good network security to keep the personal data they hold protected.

8. Data Breach

8.1 In the event of data being lost or shared in a manner that is not compliant with the school's data protection policy, it is vital that appropriate action is taken immediately to minimise any associated risk as soon as possible.

8.2 **On discovering or causing a breach, or potential breach, the staff member must immediately notify the school's Data Protection Team or headteacher in accordance with the school's Data Breach Procedure.** This must be done without undue delay. Failure to do so could have an impact

on investigating the breech and will lead to further action by the school. If a breach has occurred the school's Designated Protection Officer (DPO) will be informed.

Data Protection Officer (DPO)
Please find below details of the School's Data Protection Officer: -
Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

8.3 If the DPO decides after investigation that a data breach has occurred, they will inform the Information Commissioner's Office (ICO). This must happen within a 72 hour time frame. If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPO will also inform the head teacher and the chair of governors.

8.4 Once the breach has been resolved, the data protection team and DPO should fully review both the causes of the breach and the effectiveness of the response to it. The findings and any necessary actions should be reported to the head teacher and at the next Full Governors meeting for discussion.

8.5 It is important to take steps to reduce the possibility of personal data breaches occurring. Mandatory data protection training is in place for all staff including how to recognise and report a data breach. This is further embedded through clear and appropriate data protection policies and the regular sharing of information raising awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails

9. Photographs & Videos

9.1 The GDPR brings in stricter rules around consent, which must be given freely and openly. The school asks parents to give consent allowing the school to use photographs and videos in the following areas:

- consent for photographs/videos to be used on the school website.
- consent for photographs/videos to be used on the school's social media *(X (formerly Twitter), Instagram Facebook & YouTube)*
- Photographs and Video Consent [I give consent for photographs/videos of my child to be used in the school's termly newsletter which is distributed to parents/carers of Geoffrey Field Junior School children, celebrating the achievements and events that have occurred at the school each term.]
- Photographs and Video Consent [I give consent for photographs/videos of my child performing in whole school events, such as the Madejski Awards, Sports Day and Club Show, to be distributed to parents/carers through the school's YouTube channel.]
- Photographs and Video Consent [I give consent for photographs/videos of my child performing in class assemblies or year group performances to be distributed to parents/carers of children featuring in the performances through unlisted [non-searchable] YouTube videos.]
- Photographs and Video Consent [I give consent for photographs/videos of my child to be used to publicise the school through a school prospectus or video or advertising for school events (such as media clips, productions, fayres or other school-based events)]

Consent can be withdrawn at any time by the parent/carer. The data protection team, in consultation with the DPO if required, will decide if any further action is required in regards to previously collected, stored and shared images.
A copy of the consent request letter can be found in the appendix.

9.2 **All teaching staff** must be aware of or able to check whom the school has received parental/carer consent to use photograph/videos for the above areas. Failure to comply could put the staff member in breach of data sharing protocol and may result in disciplinary action.

9.3 "Photographs and videos of pupils that are used exclusively in the classroom area (e.g. glueing in photographs of a pupil performing a science experiment) are exempt from data protection regulation.

9.4 If a member of staff is unsure whether they require consent to share an image or video of a pupil at the school, then it is their professional duty to consult a member of the data protection team or the head teacher before sharing. Failure to do so could result in a breach of data protection regulation.

10. Request for Information

10.1 Individuals have the right to access the personal data and supplementary information you hold about them. This allows them to be aware of, and verify the lawfulness of, you processing this data.

10.2 There are three different methods for individuals or parent/carers to request information from the school regarding the data held about themselves or their child:

- **Subject Access Requests (SAR)**, which individuals can make under the General Data Protection Regulation (GDPR) to see the personal data your school holds on them (or their child, when appropriate)
- **Freedom of information (FOI)** requests, which individuals can make under the Freedom of Information Act 2000 and which allow them to request any information held by your school that isn't personal data
- **Requests by parents to see their child's educational record**, which are permitted under the Education (Pupil Information) Regulations 2005

Subject Access Requests
SARs can be made by the parent or carer of a pupil free of charge and must be complied with within 1 month on the condition that the request is founded.
The school may request two forms of identification from the person(s) requesting the data.
It is important that the person(s) making the SAR is specific about the data requested and the reasons for the requirement. Should the request be unfounded or excessive, the school may refuse to act on it or charge a reasonable fee for administration.
The school will refuse an SAR on the following grounds:

- Where it might cause serious harm to the physical or mental health of the pupil or another individual
- Where a disclosure information would conflict with safeguarding the child
- Where there are court proceedings concerning the child

Freedom of Information Requests
FOI requests must be made in writing and include a description of the information requested, even if this description is board and unclear.
FOI requests should be responded to within 20 school days from the date that the request is received. Fees for photocopying, printing and postage can be recovered from the requester.

Parental requests for data will typically fall outside FOI legislation and are more likely to be SAR or parent access requests.

Parental requests to see educational records

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

11.1 We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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

11.3 Any enquiries about the CCTV system should be directed to the school bursar (bursar@geoffreyfield-jun.reading.sch.uk)

12. Training

12.1 All staff and governors are required to undertake data protection training, informing them of all regulation changes. Data protection will also form part of continuing professional development and the induction of new staff.

12.2 Members of the Data Protection Team will also complete specific training based on the requirements of the role.

13. Monitoring

13.1 Data protection policies, procedures and breaches will be reviewed annually by the data protection team and the school's DPO.

13.2 Improvements identified in the annual audit will inform the school's action plan to improve data handling practices at the school.

13.3 The school governors will review the data protection policy annually and its approval will be sought from the full governing body.

Appendix A

Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the School are undertaking.

A Data Subject has the right to be informed by the School of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the School's sources of information obtained;

(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

· for confirmation as to whether the School process personal data about him or her and, if so

· for access to that personal data

· and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' will be a data subject access request and should be treated as such.[JC1]

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to the designated protection team who should contact Judicium as DPO in order to assist with the request and what is required.

Acknowledging the request

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the School do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;

- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
    - any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
    - any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
    - any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Fee for responding to a SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School closure periods

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because no one will be on site to comply with the request/our mail gets forwarded. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e. until a time when we receive the request), however, if we can acknowledge the request we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The School is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

· education, training or employment of the individual;

· appointment of the individual to any office; or

· provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.