

## **Right2Eat Data Protection Policy**

### **Purpose and Context**

The Right2Eat is committed to a policy of protecting individuals' right to privacy in accordance with the Data Protection Act 2018 (including any replacement of that Act) (the "DPA") incorporating the UK General Data Protection Regulation (the "GDPR", together, the "Data Protection Laws"). This policy sets out that commitment.

The Right2Eat recognizes that correct and lawful treatment of Personal Data contributes to the good reputation of the Right2Eat by demonstrating its integrity and its respect for those it deals with. The Right2Eat needs to Process certain information about its staff, students and other individuals it has dealings with. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

### **Scope**

This policy encompasses all Processing of Personal Data by staff, volunteers and affiliates, each of whom are subject to this policy. As a matter of good practice, other organizations or agents who have access to and Process Personal Data on behalf of the Right2Eat will be expected to have read and comply with this policy. It is the responsibility of the relevant Service who deal with such external third parties to ensure that such third parties agree in writing to abide by this policy, with support from published procedures and guidance, and from the Right2Eat Data Protection Team.

This policy also applies to staff and volunteers who Process Personal Data "off-site". Off-site Processing presents a

potentially greater risk of loss, theft or damage to Personal Data. Staff and volunteers should take particular care when Processing Personal Data at home or in other locations outside the Right2Eat and should comply with the Data protection regulations.

## 1. Policy Statement

1.1 This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will familiarize themselves with and act in accordance with this policy. The Right2Eat may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be managed in accordance with the Right2Eat policy framework.

Any failure to follow this policy by staff or students may result in disciplinary action. Any failure by affiliates to follow this policy may result in their access to Right2Eat IT systems and premises being restricted or removed.

## 2. Background

2.1 The purpose of the Data Protection Laws is to protect the rights and privacy of living individuals and to ensure that Personal Data is Processed fairly and transparently.

2.2 The Right2Eat collects, holds and uses Personal Data relating to individuals who have/have had a relationship with the Right2Eat. The purpose of this policy is to ensure that the Right2Eat:

2.2.1 operates procedures and practices that conform to the requirements of the Data Protection Laws when working with Personal Data;

2.2.2 clearly defines responsibilities and accountability for data protection; and

2.2.3 provides staff, researchers and students with the resources, knowledge, competencies and procedures to work with Personal Data in compliance with the Data Protection Laws and with this policy.

2.3 Breach of the Data Protection Laws can lead to enforcement action by the Information Commissioner's Office, which can now impose monetary penalties on the Right2Eat of up to £17,500,000. The Right2Eat might also be sued by any individuals affected by the breach. In addition, individuals may also be subject to fines and criminal liability where they are found to have breached the Data Protection Laws.

### 3. Data Protection Definitions

This policy tries as far as possible to avoid using technical terms. However, there are some terms used in the Data Protection Laws that it is helpful to have an understanding of in the context of data protection compliance. To assist such understanding, we have set out a list of key terms and their meanings below. Where these terms are used in this policy, they should be read and applied in this context.

#### "Data Subject"

Any living individual who is the subject of Personal Data held by an organization.

#### "Data Controller"

In the context of the majority of Personal Data held by the Right2Eat, the Right2Eat will be the Data Controller. A Data Controller is any person (or organization) who makes decisions with regard to particular Personal Data, including decisions regarding the purposes for which Personal Data is Processed and the way in which the Personal Data is Processed.

### "Personal Data"

Data relating to a living individual who can be identified from that information or from that data combined with other information in possession of the Right2Eat. Includes name, address, telephone number, volunteer or staff ID number, details of schools attended and photographs (which may also constitute Sensitive Personal Data). Also includes expression of opinion about the individual, and of the intentions of the Right2Eat in respect of that individual.

### "Process or Processing"

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### "Sensitive Personal Data"

Or "Special Categories of Personal Data" means

Personal Data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data for the purpose of uniquely identify a person (e.g. fingerprints), data concerning physical or mental health or condition (e.g. substance abuse testing), sexual life, criminal offences, or related proceedings. Any use of Sensitive Personal Data or Special Category Data must be strictly controlled in accordance with this policy.

### "Third Party"

Any individual/organization other than the Data Subject or the Data Controller (i.e. the Right2Eat) or an employee of the Right2Eat who is Processing Personal Data on behalf of the Right2Eat in accordance with this policy.

## 4. Responsibilities Under the Data Protection Laws

4.1 The Right2Eat is the Data Controller in respect of Personal Data Processed by and for the Right2Eat.

4.2 The senior post holder with overall responsibility for this policy is the Right2Eat Secretary on behalf of the Right2Eat Senior Management Team.

4.3 The Right2Eat Secretary has delegated responsibility for day-to-day data protection matters to the Right2Eat Solicitor, who has been appointed as the Data Protection Officer for the Right2Eat.

4.4 The Data Protection Officer can be contacted at [contact@theright2eat.com](mailto:contact@theright2eat.com).

4.5 An Information Governance Group (IGG) has been established to define, approve, steer and monitor Information Management (including in relation to data protection) within the Right2Eat. This includes overseeing information governance roles and responsibilities, policies and procedures and activities in order to embed compliance, promote best practice, and provide technical solutions within all services.

4.6 Senior management within the Right2Eat have overall responsibility for the Processing of Personal Data within the Right2Eat and for ensuring that such Processing is undertaken in a way that is compliant with this policy. All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the Right2Eat, but ultimately, compliance with data protection legislation is the responsibility of all members of the Right2Eat who Process Personal Data.

4.7 The Right2Eat has a designated Data Protection Champion who acts as a first point of contact for that Right2Eat relating to data protection issues. The Data Protection Champions raise awareness of data protection and information security responsibilities, policies and processes within the Right2Eat, and promote the maintenance and disposal of information held by the Right2Eat in accordance with Right2Eat policies and procedures. The Data Protection Champions are supported by the Senior Management, who will provide them with guidance, information, updates and training.

4.8 All staff are responsible for:

4.8.1 ensuring that they have undertaken Right2Eat-provided data protection training;

4.8.2 checking that any information that they provide the Right2Eat in connection with their employment is accurate and up to date and for informing the Right2Eat of any changes to their personal data (e.g. change of address); and

4.8.3 ensuring that any Personal Data Processed by them is Processed in accordance with the Data Protection Laws and with this policy.

4.9 Staff who have a responsibility for supervising/mentoring volunteers who are undertaking Processing of Personal Data (e.g. as part of a research project or on a placement) have a responsibility to ensure that the volunteer/staff is informed as to their responsibilities under the Data Protection Laws, by reference to this policy and other relevant materials. For the avoidance of doubt, volunteers or students on placement at the Right2Eat should not be given access to ASIS.

4.10 All students are responsible for checking that any information that they provide the Right2Eat in connection with their enrolment and study at the Right2Eat is accurate and up to date and for informing the Right2Eat of any changes to their Personal Data (e.g. change of address).

4.11 Volunteers/Students who are considering Processing Personal Data or data relating to service users collated as part of a qualitative research project as part of their studies must notify and seek approval from Senior Management as part of the Right2Eat approvals process. Such students/volunteers will be bound by the Data Protection Laws and by this policy and must ensure that they act in accordance with both.

## 5. Data Protection Principles

5.1 The Right2Eat policy is to Process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All staff/volunteers have personal responsibility for the practical application of the Right2Eat data protection policy.

5.2 The Right2Eat will observe the principles set out in the Data Protection Laws in respect of the Processing of Personal Data and will adhere to the following principles:

5.2.1 to Process lawfully, fairly and transparently. Those responsible for Processing Personal Data (see section 4 above) must make reasonable efforts to ensure that Data Subjects are informed of the identity of the Data Controller (i.e. the Right2Eat), the purpose(s) and legal basis of the Processing, any disclosures to third parties that are envisaged and an indication of the period for which the Personal Data will be kept.

5.2.2 to obtain personal data for specific, explicit and legitimate purposes. Personal Data will not be Processed in a manner incompatible with those purposes, and Personal Data obtained for specified purposes must not be used for a different purpose.

5.2.3 to ensure that the Personal Data is adequate, relevant and not excessive in relation to the purposes for which it is used. Information that is not strictly necessary for the purpose for which it is obtained should not be collected. If Personal Data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

5.2.4 to keep Personal Data accurate and up to date (and where inaccurate ensure they are erased and rectified



without delay). Personal Data that is kept for a long time must be reviewed and updated as necessary. No Personal Data should be kept unless it is reasonable to assume that it is accurate.

It is the responsibility of all individual staff, students and other persons to ensure that Personal Data held by the Right2Eat is accurate and up to date. Completion by a Data Subject of an appropriate registration or application form, etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the Right2Eat of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Right2Eat to ensure that any notification regarding change of circumstances is noted and acted upon.

5.2.5 not to keep Personal Data for longer than is necessary for the purposes for which it is used (see Section 14 on Retention and Disposal of Data); and

5.2.6 to keep Personal Data secure to prevent unauthorized or unlawful Processing and accidental loss, damage or destruction, using appropriate technical or organization measures. (see Section 8 on Security of Data).

5.2.7 to Process Personal Data in accordance with the rights of data subjects in accordance with the Data Protection Laws (see Section 6 on Data Subject Rights).

5.2.8 not to transfer Personal Data to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the Processing of Personal Data (see Section 15 on International Transfers).

5.3 The Right2Eat should generally not Process Personal Data unless:

5.3.1 it is to fulfil a contract with the individual (be this a student, a member of staff or a third party); or

5.3.2 the Processing is necessary to comply with the Right2Eat legal obligations or exercise legal rights; or

5.3.3 the Processing is required for a task in the public interest, or in the exercise of the Right2Eat official authority; or

5.3.4 the Processing is in the Right2Eat legitimate interests and does not unduly prejudice the individual's privacy.

5.4 To the extent the Right2Eat Processes Special Categories of Personal Data, it must ensure that such Processing satisfies the conditions for Processing required by the Data Protection Laws (see Section 7 on Special Categories of Personal Data). Transparency is key to data protection. Individuals should be told how, why and on what basis their personal data is being Processed.

5.5 Transparency is key to data protection. Individuals should be told how, why and on what basis their personal data is being Processed.

5.6 The Right2Eat will publish privacy notices in respect of its Processing of Personal Data of staff, volunteers, certain partners and visitors, which tell those people what data is collected about them, what it is used for, the legal basis for Processing the data, who it will be shared with and how long it will be held for. When gathering Personal Data or establishing new data protection activities, members of staff should check existing privacy notices to

see whether they need to be updated to reflect the new activities, or whether new privacy notices are required to cover that activity. They should also ensure that any new Processing activities are added to the Right2Eat Record of Processing Activities.

5.7 There are limited exceptions to the requirement to give Data Subjects notice of processing activities. In any case of uncertainty as to whether a notification should be given or updated, staff should contact their Data Protection Champion. In the event that staff or students Process Personal Data on behalf of another party (as a part of research activities or otherwise), due diligence should be carried out (and contractual protection obtained) to ensure appropriate data protection notices or consents have been given or obtained.

## 6. Data Subject Rights

6.1 Under the Data Protection Laws, Data Subjects have the following rights regarding the Processing of their Personal Data and the data that are recorded about them:

6.1.1 to access personal data held by the Right2Eat about them (please see Section 12); to require the Right2Eat to rectify any inaccurate personal data held by it about them; and to require the Right2Eat to erase personal data held by it about them. This right of erasure will only apply where, for example, the Right2Eat no longer needs to use the Personal Data to achieve the purpose it was collected for; or where the Data Subject withdraws their consent if the Right2Eat is using their Personal Data based on Data Subject consent; or where the Data Subject objects to the way the Right2Eat Processes their data and this is upheld;

6.1.2 to restrict the Right2Eat Processing of the Personal

Data it holds about them. This right will only apply where, for example, the Data Subject disputes the accuracy of the Personal Data the Right2Eat holds; or where they would have the right to require the Right2Eat to erase the Personal Data but would prefer that its Processing is restricted instead; or where the Right2Eat no longer needs to use the Personal Data to achieve the purpose for which it was collected, but it requires the data for the purposes of dealing with legal claims.

In cases where the Right2Eat has disclosed data to another party, and it is not disproportionate for the Right2Eat to do so, it will let the recipients of the data know that the Right2Eat has rectified, erased or restricted the Processing of it;

6.1.3 to receive personal data, which they have provided to the Right2Eat, in a structured, commonly used and machine-readable format (where Processing is automated and is either based on consent or is necessary for the performance of a contract). Data Subjects also have the right to transfer (or require the Right2Eat to transfer) this Personal Data to another organization (for example, a new employer or higher education institution);

6.1.4 to object to the Right2Eat Processing of Personal Data it holds about them (where its justification for Processing the data is either that the Processing is necessary for the performance of a task in the public interest, or for the purposes of its own legitimate interests);

6.1.5 to require a review. Data Subjects may ask the Right2Eat to review any decisions that it has made about them using automated Processing;

6.1.6 to withdraw their consent, where the Right2Eat is relying on it to Process their personal data.

6.1.7 to prevent Processing for the purposes of direct marketing;

6.2 The Right2Eat will have procedures in place to ensure that these rights can be exercised and will publicize these on its website.

6.3 If staff or students have concerns about the way in which their personal data is being used or Processed by the Right2Eat, they may contact a Data Protection Champion or the Data Protection Officer, in the first instance. If after this, they are not satisfied by the Right2Eat response they have the right to lodge a formal complaint with the Information Commissioner's Office.

## 7. Special Categories of Personal Data

7.1 Special Categories of Personal Data are afforded a higher level of protection by law. It will normally be necessary to have an individual's explicit consent to Process Special Categories of Personal Data, unless exceptional circumstances apply or the Processing is necessary to comply with a legal requirement, including to fulfil its employment duties as an employer. The consent should be a freely given (i.e. it should not be conditional), specific (i.e. it should set out exactly what is being consented to), informed, (i.e. it needs to identify the relevant data, why it is being Processed and to whom it will be disclosed) and an unambiguous indication of the individual's wishes by which they, by a statement or by a clear affirmative action (i.e. the ticking of an unticked box) signify their agreement. When relying on explicit consent as the legal basis for Processing Personal Data, there will be instructions with details of how to withdraw their consent, if they wish to do so. Staff should contact the Data Protection Officer for more information

about the conditions to be satisfied to enable Processing of Special Category Personal Data.

7.2 The Right2Eat will not rely on consent for the purposes of Processing staff Personal Data save in limited circumstances where it can be demonstrated that there is a genuine choice and the consent was freely given. If any member of the Right2Eat wishes to Process any Personal Data by relying on consent as a means to do so they must consult the Data Protection Officer for further guidance.

## 8. Security of Data

8.1 All staff are responsible for ensuring that any Personal Data (on others) which they hold are kept securely in line with the Right2Eat IT Security Policy and Procedure and in appropriate systems and that such data is not disclosed to any unauthorized third party (see Section 13 on Disclosure of Data for more detail).

All Personal Data should be accessible only to those who need to use it. A judgment should be made based upon the sensitivity and value of the information in question, but consideration should always be given to keeping Personal Data:

8.2.1 in a lockable room with controlled access;

8.2.2 in a locked drawer or filing cabinet; or

8.2.3 if computerized, password protected.

8.3 Personal Data must not be stored on removable media (such as USB storage devices, removable hard drives, CDs or DVDs) or mobile devices (laptops, tablets or smart phones) unless it is encrypted or password protected, and the key kept securely. A backup copy should also be kept on the secure Right2Eat servers. Personal Data must not be stored in generic personal cloud services such as Dropbox.

8.5 If Personal Data is transferred using removable media, a secure, tracked service must be used to ensure safe delivery.

8.6 Care should be taken to ensure that PCs and terminals are not visible except to authorized staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorized individuals.

8.7 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of Personal Data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely wiped clean before disposal. If in doubt as to what the correct security measures are for the deletion or disposal of Personal Data, advice should be taken from Right2Eat IT Support team or the individual responsible for overseeing software management.

8.8 Where the Right2Eat uses external organizations to Process Personal Data on its behalf additional security

arrangements need to be implemented in contracts with those organizations to safeguard the security of Personal Data. There are also mandatory legal protections which must be included in any contract with such parties. Any Data Processing agreement the Right2Eat enters into must contain such clauses.

8.9 In the event that the Right2Eat acts as a Data Processor (please see below), Processing personal data on behalf of a third party, such third party may require additional security arrangements to be implemented. There are also mandatory legal protections which must be included in any contract, and that needs to be flowed down to any sub-processor used by the Right2Eat.

8.10 Members of the Right2Eat should consult their line manager or the Data Protection Team to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

## 9. Reporting Breaches

9.1 Members of the Right2Eat have an obligation to report actual or potential data protection compliance failures to the Data Protection Officer immediately they become aware of them, following the published breach notification procedure. The Data Protection Laws provide that breaches must be notified to the ICO as soon as possible and in any event within 72 hours of becoming aware of them. Notification to the Data Protection Officer also allows the Right2Eat to:

9.1.1 investigate the failure and take remedial steps if necessary; and

9.1.2 make any other applicable notifications, including to



affected Data Subjects  
where appropriate.

9.2 Right2Eat staff may be required as part of their duties to support the Right2Eat in any such investigation.

9.3 Where the Right2Eat is acting as a Data Processor, it will have a responsibility to notify actual or potential data protection compliance failures to the third party it is Processing personal data on behalf of. The contract between the Right2Eat and the third party it is Processing personal data on behalf of may also have additional contractual restrictions or timescales in respect of such support/ assistance. Members of the Right2Eat should check the contractual position carefully and check with the Data Protection Officer if they are unclear how to proceed.

## 10. Acting as a Data Processor

10.1 When the Right2Eat Processes the Personal data of staff, volunteers and other individuals (in a professional or personal context) it is ordinarily the case that the Right2Eat would be known as a Data Controller. A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed.

10.2 In some limited circumstances, the Right2Eat may be a Data Processor; i.e. it is Processing the data on behalf of a third-party Data Controller.

10.3 If Members of the Right2Eat are handling Personal Data and are not sure whether the Right2Eat is acting as a

Data Controller or a Data Processor, they should contact their line manager, Data Protection Champion or the Data Protection Team in the first instance. It is key to understand the relationship, in order to determine how such personal information should be handled.

10.4 The Data Controller has the majority of the obligations under the Data Protection Laws, e.g. in respect of Data Subject rights and ensuring appropriate consents are obtained or privacy notices are given. However, a Data Processor also has a number of obligations under Data Protection Laws. In most cases, the Processing obligations imposed on the Right2Eat will be guided by the contract entered into between the Right2Eat and the third party on whose behalf it is Processing.

## 11. Accuracy, Adequacy, Relevance and Proportionality

11.1 Members of the Right2Eat should make sure data Processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal Data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

11.2 Individuals may ask the Right2Eat to correct Personal Data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Data Protection Officer.

11.3 Staff and volunteers must ensure that Personal Data

held by the Right2Eat relating to them is accurate and updated as required. If personal details or circumstances change, staff and volunteers should inform Senior Management respectively so the Right2Eat records can be updated.

## 12. Rights of Access to Personal Data

12.1 As set out above, individuals have the right (subject to certain exceptions) to request access in relation to information held by the Right2Eat about them in electronic format and/or in manual records which form part of a relevant filing system, save where exemptions apply. A request of this nature is known as a “subject access request”. All such requests should be referred immediately to the Data Protection Team. This is particularly important because the Right2Eat must respond to a valid request within the legally prescribed time limits.

12.2 Any individual who wishes to exercise this right should apply in writing (which can be by email) to the Right2Eat Data Protection Team. The Right2Eat must respond to requests without delay and in any event within one month of their receipt. In order to assist the Right2Eat Data Protection Team in complying with such requests, it is helpful to make such requests through the general enquiries page. For information on responding to subject access requests in accordance with the Data Protection Laws see the guidance

titled 'Dealing with subject access requests (SARs)' available on the <https://www.gov.uk/> website.

12.3 Where a request is made for examination scripts (where these are still held), no copies of the scripts will be provided but students may view the script in the presence of a representative from Registry. Examiners' comments can be transcribed and provided as part of a subject access request.

12.4 In order to respond efficiently to data subject rights requests the Right2Eat needs to have in place appropriate records management practices.

12.5 In addition to the above, where the Right2Eat is acting as a Data Processor, it will have a responsibility to provide assistance to the third party it is Processing Personal Data on behalf of, in respect of individuals exercising their rights. The contract between the Right2Eat and the third party it is Processing Personal Data on behalf of, may also have additional contractual restrictions or timescales in respect of such support/ assistance. You should check the contractual position carefully prior to (a) responding to a request made directly by an individual or third party, or (b) providing assistance to the third party; and check with the Data Protection Team if you are unclear how to proceed.

### 13. Disclosure of Personal Data

13.1 The Right2Eat must ensure that Personal Data is not disclosed to unauthorized third parties. This includes family members, friends, government bodies, the media, and in certain circumstances, the Police.

13.2 All Right2Eat staff should exercise caution when asked to disclose Personal Data held by the Right2Eat about

another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's personal details to someone who wished to contact them regarding a non-work-related matter, especially when such details are not otherwise publicly available (such as work contact details on the Right2Eat website). The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Right2Eat business.

13.3 This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

13.3.1 where the disclosure is in the legitimate interests of the Right2Eat (e.g. disclosure to staff – Personal Data can be disclosed to other Right2Eat employees if it is clear that those members of staff require the information to enable them to perform their jobs);

13.3.2 where the Right2Eat is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring, all of which are covered in the Right2Eat privacy notices for staff and volunteers); or

13.3.3 where disclosure of data is required for the performance of a contract (e.g. sponsor, funder, SLA etc.).

13.4 If Personal Data is to be shared with a third party in connection with the performance of a contract, then approved data protection clauses must be included in the relevant contract. The Right2Eat Data Protection Officer should be consulted on every occasion before any such contracts are entered into and Personal Data must not be shared with the third party until an appropriate contract is in place.

13.5 The Data Protection Laws permit certain disclosures without notification to the Data Subject in certain cases, so long as the information is requested for one or more of the following purposes:

13.5.1 to safeguard national security;

13.5.2 prevention or detection of crime including the apprehension or prosecution of offenders;

13.5.3 assessment or collection of tax duty;

13.5.4 discharge of regulatory functions (includes health, safety and welfare of persons at work);

13.5.5 to prevent serious harm to a third party; or

13.5.6 to protect the vital interests of the individual; this refers to life and death situations.

Requests must be supported by appropriate paperwork and should follow the agreed protocols if in place. Where a third-party request is received citing one of these grounds, the request should be passed to an authorized person within the Right2Eat for approval before any information is related. The authorized personnel are, the Right2Eat office manager or the Right2Eat Director.

13.6 When members of staff receive enquiries as to whether a named individual is a member of the Right2Eat (staff or volunteer), the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the Right2Eat may constitute an unauthorized disclosure of Personal Data.

13.7 Unless the Data Subject has requested otherwise, Personal Data should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

13.8 As an alternative to disclosing Personal Data, the Right2Eat may offer to do one of the following:

13.8.1 pass a message to the Data Subject asking them to contact the enquirer; or

13.8.2 accept a sealed envelope/incoming email message and attempt to forward it to the Data Subject.

13.9 Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Right2Eat" to avoid confirming their membership of, their presence in or their absence from the Right2Eat.

13.10 Further information regarding the disclosure of personal information can be found in the guidance titled 'Data protection' available at <https://www.gov.uk/data->

protection.

13.11 If in doubt, staff should seek advice from their line manager.

## 14. Retention and Disposal of Data

14.1 The Right2Eat discourages the retention of Personal Data for longer than it is required. Once a member of staff has left the Right2Eat or the purpose for which that data was collected has ended, it will not be necessary to retain all the information held on them. Some Personal Data will be kept for longer periods than others. The Right2Eat confidential information protocol should be followed for the retention and disposal of Personal Data.

14.2 The Right2Eat aims to reduce the duplication of personal data and will encourage as far as possible the use of definitive central sources of information for data used across the Right2Eat (e.g. contact addresses). Those with legitimate reason will have access to the Personal Data relevant for their job. Permissions granted for such access will be logged where possible and regularly reviewed.

14.3 The creation of systems and/or files which duplicate such data should be avoided; where it is inevitable every care should be taken to ensure that data maintained in subsidiary systems are fully synchronized with definitive sources, and updated frequently through secure and reliable interconnection.

### Staff

14.6 In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and



address, positions held, leaving salary. Other information relating to individual members of staff will be kept by Human Resources for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay, etc. will be retained for the statutory time period (between 3 and 6 years).

14.7 Staff personnel records are kept and maintained by Human Resources department. The Right2Eat will keep staff information where necessary for legitimate business purposes. To the extent that files of individual staff members are kept outside Human Resources, the Right2Eat should regularly review those files of in accordance with the Right2Eat confidential information protocol.

14.8 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date and should then be securely destroyed as confidential waste. Human Resources may keep a record of names of individuals that have applied, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

## Disposal of Records

14.9 Personal Data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with the Right2Eat Retention and Disposal Schedule.

## 15. International Transfers

15.1 Data must not be transferred outside of the European Economic Area (EEA) - the twenty-seven EU Member States together with Iceland, Liechtenstein and Norway -

without the explicit consent of the individual, or unless the Personal Data is adequately protected or an exemption applies.

15.2 Adequate protection can be provided if:

15.2.1 the data protection arrangements in the destination country have been approved by the ICO (there is a list of approved countries on the ICO website);

or

15.2.2 the recipient is a signatory to an ICO approved data protection regime; or

15.2.3 the recipient is bound by a contract that ensures that the Personal Data concerned will be adequately protected (for example, incorporating the Standard Contractual Clauses approved by the ICO).

15.3 Members of the Right2Eat should be particularly aware of this when contracting with a third party for the Processing of Personal Data (including for IT support, collaborative provision, or research purposes) or when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

15.4 In addition to the above, where the Right2Eat is acting as a Data Processor, the contract between it and the third party it is Processing Personal Data on behalf of may have additional contractual restrictions in respect of international transfers of such data. Members of the Right2Eat should check the contractual position carefully prior to transferring the Personal Data and check with the

Data Protection Officer if they are unclear how to proceed.

### 16.1 Publication of Right2Eat Information

16.2 When required to do so as a business need the Right2Eat may publish items that include Personal Data, and will continue to do so. These are:

16.1.3 names of all members of the Right2Eat Members Committee;

16.1.4 Staff Telephone and Email Directory;

16.1.5 Right2Eat marketing or user-led research videos or other multimedia versions of its work;

16.1.6 information in marketing material (including photographs), annual reports, staff newsletters, etc.;

16.1.7 publicity information included in public relations stories and press releases and on social media; and

16.1.8 staff information on the Right2Eat website (including photographs).

16.2 It is recognized that there might be occasions when a member of staff, a volunteer, or other party, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All

individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Right2Eat should use its reasonable endeavors to comply with the request and ensure that appropriate action is taken.

## 17. Direct Marketing

17.1 Any proposal to carry out direct marketing (i.e. marketing by email, telephone, post or any other means that is directed at a particular individual, whether they are a student, applicant, alumnus, member of staff or otherwise) must be reviewed and approved in advance by the Right2Eat Data Protection Officer in conjunction with the Central Marketing team.

17.2 Members of the Right2Eat should not send direct marketing material to someone electronically (e.g. by email, WhatsApp, social media messenger services or targeted banner ads) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their Personal Data for direct marketing purposes and should notify the relevant marketing team about any such request.

17.3 Any Company or Service that uses Personal Data for direct marketing purposes must inform Data Subjects of this at the time of collection of the relevant Personal Data and may only make direct marketing communications where the Data Subject has opted-in to receiving such communications. Data Subjects must also be given the opportunity to opt out of receiving communications at any time and measures must be put in place to prevent such communications from being sent once the Right2Eat

has received confirmation that a Data Subject has opted out.

## 18. Use of CCTV

18.1 The Right2Eat use of CCTV is regulated by a separate Code of Practice.

18.2 For reasons of personal security and to protect Right2Eat premises and the property of staff and students, close circuit television cameras are in operation in certain campus locations. This policy determines that personal data obtained during monitoring will be processed as follows:

18.2.1 any monitoring will be carried out only by a limited number of specified staff;

18.2.2 the recordings will be accessed only by Senior Management and staff or sub-contractors authorized by Senior Management;

18.2.3 personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete in line with the Right2Eat Retention and Disposal Schedule;

18.2.4 Right2Eat staff involved in monitoring will maintain confidentiality in respect of Personal Data.

## 19. Research

19.1 Personal Data collected only for the purposes of research (including work of staff and service users) must be Processed in compliance with the Data Protection Laws and in compliance with the Right2Eat Research Data Management Policy and its Research Ethics and Integrity

Policy and procedures. The Right2Eat will publish additional guidance to assist researchers in complying with these requirements.

19.2 Right2Eat staff carrying out research should note that Personal Data may be Processed for research purposes on the legal basis that the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the Right2Eat. Researchers may also rely on the bases that the Processing is necessary for scientific or historical research purposes, or that it is necessary for statistical purposes.

19.3 Where the legal bases for Processing Personal Data referred to above are available to researchers, the consent of the Data Subject is not required. However, such Processing is subject to safeguards to ensure that data is minimized (including being pseudonymized, and if possible anonymized) and that:

19.3.1 the Personal Data are not Processed to support measures or decisions with respect to particular individuals; and

19.3.2 the Data Subjects must not be caused substantial damage or substantial distress by the Processing of the Personal Data.

19.4 If the above conditions are met, together with technical and organizational safeguards to keep data secure, Personal Data Processed for research purposes may be:

19.4.1 Processed for purposes other than that for which it was originally obtained, including statistical or historical purposes; and

19.4.2 exempt from the Data Subject's right of access and rectification, as well as their right to restrict or object to Processing.

19.5 Other than this, Data Protection Laws apply in full in respect of academic research. The obligations to collect only necessary and accurate Personal Data, to hold Personal Data securely and confidentially and not to disclose Personal Data except in accordance with the Data Protection Laws (including in relation to publication) must all still be complied with.

## Publication

19.6 Researchers should ensure that the results of research are anonymized when published and that no information is published that would allow individuals to be identified (including where anonymized data could be matched with other data to link back to an identifiable individual) where consent has not been obtained for such use from the Data Subject or, where the nature of the research makes it impracticable or otherwise, undesirable to attempt to seek/obtain consent, that there is a legitimate interest in publication and publication would not unfairly damage the rights and freedoms of the Data Subject.

## 20. Data Protection Impact Assessment

20.1 The Right2Eat encourages all staff to incorporate

'Privacy by Design' into their activities which involve Processing Personal Data - an approach by which data protection is built into a project from the outset, and not bolted on at the end. The Privacy Impact Assessment ("PIA") is a method by which the Right2Eat can assess and address the risk of Processing and identify measures to support Data Protection.

20.2 The PIA involves setting out the envisaged Processing, its purposes, and the legal basis under which it is to be processed. It involves an assessment of the risks posed by the Processing to the rights and freedoms of the Data Subjects, and the measures to be taken to address those risks. It will include an analysis of safeguards being put in place, and will demonstrate how the Processing will be compliant with the Data Protection Laws. Once the University has carried out a PIA, it will keep it under regular review to ensure that the assessment of risk addresses circumstances as they change.

20.3 To help the Right2Eat meet its data protection obligations and to meet staff expectations of privacy, the Right2Eat carries out PIAs prior to beginning any new Processing activities where these are only required under Data Protection Laws for the large-scale Processing of Sensitive Personal Data, systematic monitoring of a public area on a large scale, the systematic evaluation of individuals based on automated Processing, and other Processing activities which are likely to result in a high risk to the rights of Data Subjects. It is good practice to carry out PIAs when embarking on new projects involving the Processing of Personal Data and staff are encouraged to do so, however where this is not the case, staff are still encouraged to consider Data Protection compliance which starting any



new Processing activity, to ensure it is conducted in line with this policy.

20.4 The data protection regulator in the UK also requires PIAs to be carried out where an organization plans a number of specific Processing activities, including using new technology, processing biometric data or collecting Personal Data from a source other than the Data Subject without providing them with a privacy notice.

21 For further guidance or advice on the Data Protection Laws or this policy and its application, please contact the Right2Eat Data Protection Officer by email at [contact@theright2eat.com](mailto:contact@theright2eat.com)