Kraft Heinz

General Data Protection Policy - PROVISIONAL

Title	**General Data Protection Policy**	Policy Owner	Data Privacy
Date of Issue	22 May 2018	Effective Date	25 May 2018
Supersedes		Dated	
		Dated	

NB. At the date of issue this Policy was still pending confirmation by Works Councils in some Kraft Heinz companies.

POLICY SNAPSHOT

GENERAL RULE

All Staff engaged by Kraft Heinz companies have a duty to handle Personal Data in accordance with Data Protection Laws.

This Policy set outs out both the responsibilities of Staff when handling Personal Data and their rights in respect of their own Personal Data

For further information, please read the full contents of this Policy.

Policy Contents

EXPLANATORY NOTES 1
A. Purpose of this Data Protection Policy 1
B. Scope 1
C. Background 1
D. Data Protection Laws 1
E. Special Category Data 1
F. Forms in which Personal Data can be held 2
G. Definitions 2
H. Structure of this Policy 3
I. Status of this Policy 3
PART A – KRAFT HEINZ'S RESPONSIBILITY TO YOU UNDER DATA PROTECTION LAWS 4
1. Data Privacy Team 4
2. General Basis for Holding Personal Data 4
3. Staff Personal Data that Kraft Heinz May Hold or Process 4
4. Third Party Personal Data Provided by Staff 4
5. How Kraft Heinz May Process Staff Personal Data 4
6. Retention of Records 5
7. Monitoring 6
7.1. Monitoring of Kraft Heinz's Systems 6
7.2. Permitted Personal Use 6
7.3. Unmonitored Personal Use 6
7.4. Systems Equipment 6
7.5. Your Use of Systems 7
7.6. Investigating Potential Misuse of Systems 7
7.7. CCTV 7
8. Your Personal Data Rights 8
9. Concerns & Complaints about your Personal Data 8
PART B - YOUR RESPONSIBILITIES TO OTHERS UNDER DATA PROTECTION LAWS 9
10. Data Protection Principles 9
11. Keeping Data Secure 10
11.1. Systems Security 10
11.2. Access to Data Stored Electronically 10
11.3. Security of Portable Devices 10
11.4. On-Site Security of Paper Copies of Personal Data 11
11.5. Off-Site Security of Paper Copies of Personal Data and other Information 11
11.6. Use of Memory Sticks and other Portable Media 11
11.7. Restrictions On Use of Unauthorised Devices or Software 12
11.8. Third-Party Access 12
11.9. Back-up of Personal Data 12
11.10. Disposal of Personal Data 13
11.11. Email Security 13
11.12. Permitted Personal Use 13
11.13. Handling Customer Contact Details 13
12. Reporting Suspected Data Security Breaches 14
13. Ensuing Individuals Know How Their Personal Data Will Be Used by Kraft Heinz 15
14. Ensuring That Personal Data Is Accurate and Kept Up to Date 15
15. Individual Rights 15
16. Requests for Access to Personal Data 15
17. Data Privacy Impact Assessments 15
18. Securely Disposing of Personal Data 15

19. Training 15
20. Data Protection and Disciplinary Action 15
21. Policy Language 16
22. Monitoring and Review of This Policy 16

APPENDICES

Appendix 1A: Kraft Heinz Europe: Employing Companies

Appendix 1B: Kraft Heinz Europe Other Current or Former Trading Companies

Appendix 2: Typesof Staff Personal Data Kraft Heinz May Process

Appendix 3: Processing of Staff Personal Data

Appendix 4: Types of Third Party Personal Data Kraft Heinz May Process

Appendix 5: Processing of Third Party Personal Data

EXPLANATORY NOTES

A. Purpose of this Data Protection Policy

The purpose of this Policy is to set out Kraft Heinz's core data protection policies applicable to all Staff who handle Personal Data for Kraft Heinz or who provide their own Personal Data to Kraft Heinz.

The Policy is intended to assist both Kraft Heinz and Staff in complying with Data Protection Laws.

See Appendix 1A for a list of Kraft Heinz's European employing and trading companies.

B. Scope

This Policy applies to all Staff who handle or provide Personal Data including Staff located outside the European Union who also handle Personal Data.

This Policy covers Personal Data held in electronic form, as well as physical data held within a structured and organised manual filing system.

Where applicable, local laws and regulations which are in addition to Data Protection Laws must also be observed. Any variations to this Policy required as a result of specific national laws will be set out in a schedule for the Kraft Heinz company affected.

C. Background

Kraft Heinz needs to collect and process Personal Date in order to run its businesses effectively and comply with its legal obligations.

The GDPR established a new framework for the collection, processing and protection of Personal Data. It is the responsibility of each member of Staff to ensure that at all times when handling Personal Data, they fully comply with all of the requirements of this Policy and with such directions as Kraft Heinz may from time to time give in relation to Personal Data.

Kraft Heinz considers its own compliance with Data Protection Laws to be crucial to both its corporate values and the success of its business. Kraft Heinz's compliance with Data Protection Law depends on Staff acting in accordance Data Protection Law and, in accordance with the spirit of GDPR, Kraft Heinz expects its Staff to treat other people's Personal Data with at least the degree of care that they would apply to their own Personal Data.

Given the importance of protecting Personal Data, breaches of this Policy will be treated as a potentially very serious matter and may result in disciplinary action, up to and including termination of employment with immediate effect where that is appropriate and permitted by the applicable disciplinary policy.

D. Data Protection Laws

Data Protection Laws include a number of different European laws that govern the way in which Kraft Heinz may process Personal Data. They also provide Data Subjects with various rights and set out what happens if the laws are not followed, including the very significant fines that can be imposed for Data Protection Law violations.

As well as dealing with an individual's rights in respect of their Personal Data, Data Protection Laws also cover other areas such as marketing and use of on-line tracking technologies, such as cookies.

This means that Data Protection Laws apply to a very wide range of our activities, including not just Kraft Heinz's own activities but also activities we have outsourced to external suppliers.

E. Special Category Data

Whilst ordinary Personal Data needs to be handled with care, certain classes of particularly sensitive information, known as "**Special Category Data**", require even greater care. Kraft Heinz will handle Special Category Data with appropriate care and requires Staff to do the same.

F. Forms in which Personal Data can be held

Data Protection Laws apply not just to Personal Data held electronically but also cover Personal Data which is held on paper and other physical forms and kept in well-structured manual filing systems.

Images, such as photographs and CCTV footage, can also be Personal Data, as can audio recordings and location data that can be linked to an individual.

G. Definitions

"**Data Protection Laws**" include the GDPR and other applicable privacy and data protection laws.

"**Data Subject"** means a person who is the subject of Personal Data.

"**DPIA**" means a Data Privacy Impact Assessment.

"**EEA**" means the European Economic Area as at 25 May 2018 and save where expressly stated otherwise will continue to include the United Kingdom at any time after that date regardless of whether or not the United Kingdom is a member of the European Union at the time.

"**GDPR**" means the General Data Protection Regulation

"**Kraft Heinz**"/ "**we**" means any Kraft Heinz company which is collecting or processing Personal Data. In relation to Part A of this Policy, unless otherwise stated 'Kraft Heinz' means the legal entities which are listed in Appendix 1A.

"**Media**" means any portable device capable of storing, transferring, manipulating or removing data and includes but is not restricted to mobile devices, flash memory devices (drives, disks, cards etc.) removable hard drives and optical media (CDs, DVDs etc.).

"**Permitted Personal Use**" means reasonable Personal Use as further set out in this Policy and our Systems Use policy.

"**Personal Data**" is any information relating to an identified or identifiable living person who is in the EU (or who is otherwise within the scope of the GDPR, or any legislation enacting the GDPR, from time to time).

The definition of Personal Data is very broad and can include not just a Data Subject's email and physical addresses but also their online activity, biographical information and health/fitness data.

Kraft Heinz collects and processes both Staff Personal Data and Third Party Personal Data.

Unless otherwise stated references in this Policy to 'Personal Data' include both Staff Personal Data and Third Party Personal Data.

"**Personal Use**" means any use of the Systems by Staff for personal purposes.

"**SAR**" means 'subject access request' and refers to a Data Subject's right to have access to their Personal Data.

"**Special Category Data**" is Personal Data concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic and biometric identification data and, for the purposes of this Policy, criminal convictions and offences.

In this Policy, references to "**Personal Data**" also include Special Category Data unless otherwise stated.

"**Staff**"/"**you**" means permanent and temporary employees, workers and contractors undertaking activities for and at the direction of any Kraft Heinz company where those Staff handle Personal Data for Kraft Heinz.

"**Staff Personal Data**" means Personal Data where the Data Subject is a Staff member.

"**Systems**" means Kraft Heinz information technology and communications systems and networks and the equipment associated with or connected to those networks including mobile devices.

"**Third Party Personal Data**" means Personal Data of Data Subjects who are not Staff.

H. Structure of this Policy

Part A of this Policy sets out how we will handle Staff Personal Data.

Part B gives guidance on some of the key measures that Staff are required to follow, when dealing with all Personal Data.

This Policy also sets out Kraft Heinz's rules on data protection and the conditions that must be satisfied in relation to obtaining, handling, processing, storing, transporting and destroying Personal Data.

I. Status of this Policy

Staff are required to fully comply with this Policy at all times when they are using Systems, whether for business or Personal Use.

This Policy has been provided to Works Councils or other consultative bodies for consultation or agreement as required by applicable law in the relevant location.

This Policy does not form part of any member of Staff's contract of employment or engagement and we may amend it at any time, subject to any applicable legal requirements.

This Policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by regulatory authorities and industry standards.

PART A – Kraft Heinz's responsibility to You under Data Protection Laws

This section of the Policy sets out how your Personal Data will be used, including by the member(s) of the Kraft Heinz group that you are employed or engaged by.

1. Data Privacy Team

Kraft Heinz has appointed a Data Privacy Team to help it comply with its obligations under the Data Protection Laws. The key roles of the Data Privacy Team are as follows:

- to provide a point of contact and support for Staff;
- to carry out and support the carrying out of DPIAs;
- to provide training to staff;
- to liaise with the local data protection authority; and
- to deal with SARs and other Data Subject rights under GDPR;

If you have any queries about the way in which you should handle Personal Data, please contact the Data Privacy Team. Their email address is: GDPR@kraftheinz.com

If you are unable to contact the Data Privacy Team in an emergency, please contact Legal.

2. General Basis for Holding Personal Data

In most cases Kraft Heinz will hold Staff Personal Data because it is (i) necessary for performance of a contract; (ii) is necessary to meet legal obligations; or (iii) is held in connection with a legitimate interest of Kraft Heinz (unless overridden by others' rights or interests).

In situations where Kraft Heinz holds your Personal Data on the basis of your consent, we will seek that consent from you. You are entitled to refuse to give that consent and to withdraw it at any time, once given (for the avoidance of doubt such withdrawal will not have retrospective effect in relation to previous processing).

The above is only intended to be a broad summary and please see the rest of this Policy for detailed information on how Kraft Heinz deals with Personal Date and your Personal Data rights

3. Staff Personal Data that Kraft Heinz May Hold or Process

For the types of Staff Personal Data that Kraft Heinz may hold please see Appendix 2.

4. Third Party Personal Data Provided by Staff

We may collect and process Personal Data about your next of kin or other family members so that they can be contacted in an emergency.

In addition, where you nominate someone as a beneficiary under any benefits we provide to you (for example pensions, health insurance, use of a company car etc.) we may also process that person's Personal Data if it is required for, or in connection with, the operation and administration of that benefit. You will be responsible ensuring that you have permission to provide your beneficiary's Personal Data to us and for letting us know, if it changes.

In all cases, Personal Data relating to third parties will also be processed in accordance with the Data Protection Laws and as described in this Policy.

5. How Kraft Heinz May Process Staff Personal Data

Kraft Heinz may only process Personal Data for lawful purposes.

We will undertake a number of processing activities in relation to Staff Personal Data and for examples of the type of data processing we may undertake please see Appendix 3.

In order to fulfil our legal and other obligations and in connection with our rights including protection of our legitimate interest, we reserve the right to disclose Personal Data (or Special Category Data as appropriate) to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administrative purposes (for example, HM Revenue and Customs in the UK) and to the extent that local law allows and/or requires this.

Where necessary we may also provide Personal Data to contractors and suppliers who provide services to us, including assistance with the processing activities set out in Appendix 3. In such cases, we will enter into a data processing agreement (including provisions required by GDPR) with the contractors and suppliers to whom we provide Personal Data.

We may transfer Personal Data to other Kraft Heinz Group companies, partners, suppliers, law enforcement agencies and to other organisations that are located outside the EEA for the purposes of:

- HR administration (for example, staff recruitment and planning);
- payroll processing and administration;
- Benefits processing and administration;
- staff secondment;
- staff relocation;
- visa applications;
- management of staff engaged by companies outside the EEA;
- taxation and registrations for staff working outside the EEA;
- fulfilling our legal requirements/obligations;
- fulfilling customer contracts;
- overseas legal proceedings;
- Systems operation and management;
- outsourcing;
- Kraft Heinz business travel; and
- as reasonably required for the proper operation of Kraft Heinz's business;

The laws of some jurisdictions outside the EEA may not be as protective as Data Protection Laws in the EEA. Kraft Heinz will ensure that, for such jurisdictions, appropriate measures are in place for compliance with Data Protection Law in relation to transfer of Personal Data to those jurisdictions.

6. Retention of Records

We have legal duties to keep various records and those records need to be held for different periods of time, depending on their contents (see the Kraft Heinz Data Retention policy for details).

We will therefore keep Personal Data for as long as we reasonable consider may be needed in connection with those obligations.

Where we do not have keep Personal Data for a period specified by law we will not keep Personal Data for longer than may be permitted by Data Protection Law.

For further information about our approach to data retention, please see Kraft Heinz's Data Retention policy.

7. Monitoring

7.1. Monitoring of Kraft Heinz's Systems

Kraft Heinz's Systems, are provided for business use and with the intention of promoting effective communication and working practices within our organisation.

In order to manage use and operation of the Systems and to maintain IT and Personal Data security, use and operation of the Systems (including telephone (mobile and fixed) and computer systems, including email and internet access) may be monitored with the resulting records being retained and used for those purposes. Such monitoring which, where practicable, will be undertaken by automated means, is intended to assist with management and operation of the System and to protect Systems and Personal Data security. It is not intended or designed to breach any legitimate privacy rights Staff may have.

Specific monitoring of individual members of Staff is only carried out if and to the extent that it is permitted or required by law, and where Kraft Heinz considers it is both necessary and justifiable for business purposes.

The telephone Systems used by Kraft Heinz allows identification and recording of all dialled numbers, received calls and call durations. Such records may be retained and used as permitted by applicable law, typically for security, management and operational purposes, including call billing.

The content of telephone calls will only be recorded where and to the extent the recording is permitted by local law and Kraft Heinz considers that such recording is appropriate. Kraft Heinz will advise Staff where telephone call content is recorded as a matter of normal routine.

Any log files generated will be retained for a reasonable period (and in any event no longer than is permitted by law) so that instances of attempted misuse and other security events can be detected and investigated, with follow up actions being taken where necessary.

Where breaches of this Policy are identified then, to the extent permitted by law, appropriate action may be taken. Subject to the applicable disciplinary policy, this may include action up to and including dismissal with immediate effect.

7.2. Permitted Personal Use

Please note that whilst reasonable care will be taken to ensure that we do not compromise your privacy when you engage in Permitted Personal Use, facilities to use Systems without any form of monitoring at all are not generally available. We are therefore unable to guarantee that Permitted Personal Use will not be monitored in any circumstances and you should not assume that where you chose to engage in Permitted Personal Use using Systems that use will remain entirely private to you at all times and in all circumstances (for example, the System will automatically retain details of addresses to which emails are sent and also details of URLs accessed).

7.3. Unmonitored Personal Use

It is suggested that Staff wishing to undertake unmonitored Personal Use do so using their own personal devices which connect directly to the internet. Staff should be aware that Permitted Personal Use which takes place using Kraft Heinz Wi-Fi will be subject to the normal Systems operation and security monitoring.

7.4. Systems Equipment

All Systems equipment (in particular computers and mobile/smartphones) which we provide to Staff is intended for professional use only. Whilst Staff may use Systems equipment for Permitted Personal Use it is not provided for that purpose.

We reserve the right to require the immediate return of Systems equipment supplied by us and to retrieve from any equipment used in connection with Kraft Heinz's business of data on that equipment including but not limited to the contents of messages (including but not limited to emails, voicemail,

SMS and other forms of electronic messaging) and the results of internet and other online searches and data resulting from them where the same are relevant to Kraft Heinz's business. Such data may be used for the following purposes:

a) as required for proper conduct of Kraft Heinz's business including record keeping;

b) where necessary for the purposes of the legitimate interests pursued by Kraft Heinz;

c) monitoring whether the use of the email system or the internet is legitimate and in accordance with this Policy including Permitted Personal Use (you acknowledge that Kraft Heinz can use software to monitor the identity of senders and receivers of emails);

d) finding lost messages or to retrieve messages lost due to computer failure;

e) assisting in the investigation of and response to wrongful acts, including those which may breach this or any of our other policies including Permitted Personal Use or any applicable law; and

f) complying with any legal obligation.

7.5. Your Use of Systems

It is a condition of your use of the Systems that at times while you are using them you:

a) strictly comply with your authorisation to use the Systems;

b) behave in a professional manner;

c) do not do anything which might bring the good name of Kraft Heinz or any of its companies into disrepute;

d) do not circulate any material that might reasonably cause offence to others, including any material of a violent, harassing, racist, sexist or criminal nature;

e) do not otherwise behave in an inappropriate way in relation to your colleagues and others whom you contact using the Systems; and

f) do not seek to use the Systems for any unauthorised use or purpose including attempting to access any material or systems (including those belonging to any third party) you are not authorised to access.

For further details, please see the Systems Use policy

7.6. Investigating Potential Misuse of Systems

Breaches of this Policy (which include misuse of the Systems) will be considered a potentially serious matter and if evidence of a breach of this Policy or of misuse of the Systems is found or we have a reasonable suspicion that such breach, misuse or any activity which is illegal or in breach of any Kraft Heinz policy has occurred, we may undertake a more detailed investigation in accordance with our disciplinary procedures and applicable laws.

Such investigations may include the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure where such examination and disclosure is permitted by law.

If necessary, information identified during such investigations may be handed to the police or other law enforcement agency. Investigations and disclosure of information to the relevant authorities will be carried out only to the extent permitted by law.

Misuse of the Systems may result in appropriate disciplinary action up to and including dismissal with immediate effect being taken against you. We also fully reserve any other legal right we might have in respect of such failure.

7.7. CCTV

Some of Kraft Heinz's buildings and sites use CCTV systems to monitor their exteriors and/or interiors for security reasons, in the interests of health and safety or for remote process observation. CCTV data is normally recorded and retained for a limited period.

Use of CCTV and recording of CCTV data is only carried out in accordance with Kraft Heinz's CCTV policy.

8. Your Personal Data Rights

Under Data Protection Laws Staff are entitled to ask Kraft Heinz for a copy of their Personal Data and to ask for it to be corrected, edited or have its processing restricted. Staff are also entitled to ask Kraft Heinz to transfer some of their information to other organisations.

Staff may also have rights to object to some processing of their Personal Data although Kraft Heinz may continue that processing if it is required in connection with legal obligations. Where Kraft Heinz has asked Staff for their consent to process Personal Data and that consent is withdrawn we will not process that Personal Data further but may not be able to continue providing the service for which the Personal Data was sought.

Staff Personal Data rights may be limited in some situations, for example, where Kraft Heinz demonstrates that it has a legal requirement to process your data, such as where tax authorities require us to retain it or where it is needed for proper performance of a contract. Where Kraft Heinz has a legal right or obligation to retain Personal Data or wishes to do so in connection with its legitimate interests Kraft Heinz may retain Personal Data even if you have withdrawn consent you may have given for Kraft Heinz to hold your Personal Data.

Where Kraft Heinz requires Personal Data to comply with legal or contractual obligations, the provision of such data is mandatory. If such data is not provided Kraft Heinz will not be able to manage the employment or engagement relationship, or to meet obligations placed on it. In all other cases, provision of requested Personal Data is optional.

For any concerns or questions about how Kraft Heinz processes your Personal Data or have any questions in relation to your rights in respect of your Personal Data, please contact the Data Privacy Team.

9. Concerns & Complaints about your Personal Data

If you believe that another person may have infringed your data protection rights, you should bring that to the attention of the Data Privacy Team and also your line manager or such other person as may be specified in your business unit/local grievance procedures.

In the first instance Staff should raise all data concerns with the Data Privacy Team but Staff also have the right to complain directly to data protection authorities at any time. The relevant data protection authority will be the supervisory authority in the same country as your employing entity. Pease see here for details of national data protection authorities.

PART B - Your Responsibilities to Others under Data Protection Laws

This part of the Policy is intended to inform Staff about how they should handle Personal Data in certain circumstances.

To meet its obligations under Data Protection Law Kraft Heinz needs each and every member of Staff to fully comply with this Policy and Data Protection Law to the extent that they are personally applicable to Staff.

It is important that Staff are aware of their own data protection responsibilities towards others under the Data Protection Laws. Those responsibilities include the requirement to follow the guidelines and processes set out below.

Here are some key points to remember:

- Consider your responsibilities under the Data Protection Laws and this Policy and how they impact on your day-to-day activities.
- Only share Personal Data on a need to know basis. Don't share an entire database where only a part of it is needed.
- Double check recipient's details before sharing Personal Data. Are you sending data as intended or putting Kraft Heinz at risk?
- Use password protection for documents and files, wherever appropriate.
- Only use Personal Data in the way that the individual concerned has agreed to or as set out in this Policy.
- Always ensure that, when disposing of Personal Data, you do so securely - for example, paper documents must be put into Confidential Waste or shredded, they must not be placed in general waste.
- Treat all Personal Data with care and do not do anything to other people's Personal Data that you would not be happy to have done to your own Personal Data.

This section is intended to provide general guidance only and is not a comprehensive guide. Depending on the precise nature of your job, Data Protection Laws may mean you have additional responsibilities and obligations.

Your general responsibilities are as follows:

10. Data Protection Principles

When processing any Personal Data both Kraft Heinz and its Staff must adhere to certain data protection principles contained within the Data Protection Laws. These include the requirements that Personal Data must:

a) be processed fairly and lawfully;

b) be processed only for one or more specified and lawful purposes, and not further processed in any manner incompatible with such purposes unless expressly permitted under applicable laws;

c) be adequate, relevant and not excessive in relation to the purposes for which they are processed;

d) be accurate and, where necessary, kept up to date;

e) be kept no longer than is necessary for the purposes for which it was processed (see Retention Policy);

f) be processed in accordance with an individual's rights including, in certain circumstances, rights to access Personal Data; to have Personal Data ported to a third party; to have Personal Data corrected or erased if it is inaccurate or no longer required; and not to be subject to significant automated decision making processes where this is objected to;

g) be kept secure; and

h) only be transferred to or accessed from a country outside the EEA if that country has adequate protection of Personal Data or where there are adequate contractual safeguards to protect Personal Data.

11. Keeping Data Secure

This section 11 and section 12 (Reporting Suspected Data Security Breaches) relate not only to Personal Data but also to all information, IT and communications systems. You are responsible for ensuring that your actions do not compromise the security of the Systems and for taking appropriate care of the equipment allocated to and/or used by you. You must not allow the Systems or to be used by anyone else, other than in accordance with this Policy or as directed by Kraft Heinz.

11.1. Systems Security

a) All Systems users will be given unique account details. You must not share accounts or passwords, disclose your account details to other or use accounts not assigned to you.

b) You should always lock, logoff or shut down your PC, laptop or other devices during periods when you will be leaving them unattended (e.g. to attend meetings or during lunch breaks). Kraft Heinz's Systems equipment is, where possible, programmed to automatically lock or terminate after a designated period of inactivity and you must not seek to disable that function.

c) At the end of each working day you should ensure that your computer and other devices used by you are properly shutdown and that your monitor is switched off. If you have a laptop, you must either keep it with you or ensure that it is stored securely, for example in a locked cabinet or drawer.

d) You must ensure that Personal Data and confidential information on your screen cannot be easily read by people around you, wherever you are.

e) You must use a strong password (e.g. a mixture of capital and lower case letters, numbers and special characters) and keep it confidential. You should change it regularly and if you believe someone knows your password, you must change it immediately.

f) Alterations to or maintenance of your computer or any other Systems equipment or the installation of any hardware or software on Kraft Heinz supported assets is to only be undertaken by members of IT, or other people who are expressly authorised by Kraft Heinz to do so as part of their job role.

11.2. Access to Data Stored Electronically

a) Use passwords to restrict access to sensitive files and Personal Data.

b) Do not try to circumvent any established security procedures or authorisation levels.

c) Keep an audit trail of amendments made to databases or documents containing sensitive information.

d) You must not prevent any scheduled IT back-up processes or any malware detection or other security processes.

11.3. Security of Portable Devices

a) If you have been given access to Kraft Heinz Systems equipment, including laptops, cell phones and other portable devices, you are responsible for the safekeeping of that equipment and for taking reasonable steps to ensure it is not used by unauthorised persons, or lost, stolen or damaged. This is especially so when you are travelling or otherwise out of the office.

b) Portable devices should not be left in vehicles at any time, particularly overnight. However, if it is absolutely necessary to do so, you must make sure that they are kept out of sight.

c) If you are using a portable device in public place, such as on a train or flight, at an airport or in a hotel foyer, you must be aware of people around you and take precautions to ensure that they cannot read your screen.

d) If you use your portable device on any external or third party network, you need to ensure that network is secure and you should not use public Wi-Fi (for example, open Wi-Fi available in a hotel, airport or coffee shop) to transmit sensitive information or Personal Data. If you have any doubts about the security of a network, you should not connect your device to it.

e) You must not attempt to circumvent any encryption software or security features on portable devices.

f) Kraft Heinz uses a combination of the following security features on portable devices to ensure that they are kept secure. These include:

- user names/passwords and PIN numbers;
- anti-virus protection;
- data encryption;
- account lock out following failed access attempts;
- device/application lock following inactivity;
- account or device lock out following theft/loss;
- monitoring of use; and
- deletion of content (which may include Staff's private data) on lost or stolen devices.

11.4. On-Site Security of Paper Copies of Personal Data

a) Keep your desk clear of Personal Data and business sensitive confidential information.

b) Do not leave Personal Data or business sensitive confidential information unsecured at any time.

c) If you are printing sensitive Personal Data or business sensitive confidential information, make sure that you do not leave any of it on a printer.

d) Do not leave Personal Data or business sensitive confidential information in meeting rooms or other areas of the office. If you no longer need them, take them with you and dispose of them securely. You should also wipe white boards and similar clean before leaving meetings rooms unless clearly instructed not to do so.

e) You must ensure that Personal Data and business sensitive confidential information is held in a secure place overnight, such as a lockable filing cabinet or drawer; or in a restricted access or locked area/room.

f) You must follow any specific guidance relating to your location, department or the information concerned.

11.5. Off-Site Security of Paper Copies of Personal Data and other Information

a) Only take Personal Data or sensitive or confidential information outside the office or off-site if it is absolutely necessary.

b) Be aware of the risks of loss or theft and take appropriate precautions to make sure Personal Data and other information is kept secure.

c) Do not leave Personal Data or other sensitive or confidential information unattended at any time on trains or other public transport or in other public places and make sure that information cannot easily be seen by people around you, when you are in a public place.

d) Only store or archive Personal Data or business information off-site using a Kraft Heinz approved supplier with whom a written contract is in place.

11.6. Use of Memory Sticks and other Portable Media

Personal Data and other information may only be transferred from Kraft Heinz's Systems to any portable/removable Media where there is a genuine business justification for doing so and provided that the provisions of this Policy and directions from the Data Privacy Team are fully followed.

a) Kraft Heinz may as permitted by law monitor all copying of information from its Systems, in order to detect unauthorised data transfer and prevent security breaches.

b) The exchange of information either internally or with external parties should always be via Kraft Heinz Systems, such as email or shared data areas. Media should only be used for data transfer when a more secure alternative is not available.

c) Any Media physically transferred between Kraft Heinz and/or any third party must be sent by tracked delivery (to ensure that the Media can be tracked and recovered if lost) and the Media must be password protected and/or encrypted, with the password or key sent separately.

d) All use of Media is subject to the following:

- You may only use Media that has been purchased through or authorised by IT or the Data Privacy Team and encrypted;
- Media must be scanned for malware/virus infection using virus scanning and other software provided by IT prior to use and not used if found to carry a potential infection;
- Only store on Media data that is absolutely necessary, i.e. do not download an entire database if only small sections of it are required;
- Check that the Media you intend to use can encrypt the Personal Data and other information stored on it;
- Ensure that files held on the Media are password protected with the password being sent separately to the encrypted Media;
- Immediately delete data from the Media once it is no longer required; and
- Non-reusable Media must to be correctly disposed/destroyed at the end of its required lifecycle in accordance with the Data Privacy Team's recommendations.

11.7. Restrictions On Use of Unauthorised Devices or Software

a) Hardware that is not supplied and/or managed by IT (e.g. personal or third party laptops, tablets, smart phones, mobile phones, memory sticks etc.) cannot be connected to or installed on Kraft Heinz Systems without express permission from IT or the Data Privacy Team or as permitted by any Kraft Heinz 'Bring Your Own Device' policy.

b) You may only download and/or install software where you are expressly authorised to do so by IT. Unapproved software may contain viruses or other malware which could compromise our Systems and breach of this section 12.7(b) may result in disciplinary action which, subject to the applicable disciplinary policy, may include action up to and including dismissal without notice.

11.8. Third-Party Access

a) Kraft Heinz is responsible for the acts and omissions of its suppliers and contractors who may access or process Personal Data on its behalf.

b) If you are engaging contractors, consultants and temporary staff who have access to Kraft Heinz's Systems and/or Personal Data, they must first sign an agreement containing provisions that adequately protect Personal Data for which Kraft Heinz is responsible and you must involve Procurement in the discussions and contract negotiations.

c) In particular, any project involving the connection by a third party/supplier to Kraft Heinz's Systems will require a specific assessment of the risks and additional contractual terms relating to security.

d) All changes to third party/supplier access to Kraft Heinz's Systems must be reviewed and documented, to ensure that security is maintained.

e) If a third party access to Personal Data is no longer required, connectivity must be terminated and any Personal Data obtained by the third party must be returned or destroyed in accordance with the contractual terms.

f) All third parties with access to Personal Data must be required to notify Kraft Heinz, via their primary point of contact, of all potential and actual information security incidents experienced by themselves or their customers as soon as reasonably practicable after they become aware of eth incident.

11.9. Back-up of Personal Data

a) Wherever possible Personal Data should be held in networked storage as this can easily be backed up using automated processes.

b) Removable Media should not be used for storing business critical information as it will not be backed up and therefore will not be recoverable if lost, corrupted or accidentally deleted.

11.10. Disposal of Personal Data

a) Personal Data in paper form must be disposed of using confidential waste bins or paper shredders. If a confidential waste or a shredder is not available, please contact the facilities manager at your specific site/location/building for collection arrangements.

b) Ensure any IT hardware, mobile devices, mobile storage media or other equipment is properly cleansed of all Personal Data before disposal.

c) Non-reusable media such as CD-ROMs must be correctly disposed of or destroyed at the end of its required lifecycle.

Contact the Data Privacy team to ensure that 12.10 (b) and (c) are carried out correctly.

11.11. Email Security

a) You must not attempt to avoid or disable any virus or malware protection software,

b) You must exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious (for example, if it or any attachment has a name ending in .exe).

c) The Data Privacy team must be informed immediately if a suspected virus is received or identified.

d) We reserve the right to block access to email attachments for the purpose of effective use and/or protection of the Systems and for compliance with this Policy.

e) We also expressly reserve the right not to transmit (either in-bound or out-bound) any email message that we believe may contain a virus or other malware. This includes email sent as part of Permitted Personal Use.

f) All email traffic related to business activities must be conducted through an approved Kraft Heinz System.

11.12. Permitted Personal Use

Kraft Heinz permits limited use of its internet, email and telephone systems for Permitted Personal Use subject to certain conditions set out below and its Systems Use policy.

a) Whilst it is not our policy to undertake routine active monitoring of Personal Use, the Systems are intended for business purposes and are monitored for business reasons as permitted by law and further set out above. The Systems are neither intended nor configured for unmonitored Personal Use and Kraft Heinz is not under any obligation to alter the Systems so as to permit Personal Use that is entirely unmonitored.

b) We reserve the right to withdraw at any time the Permitted Personal Use privilege for users who abuse Personal Use by prohibited, inappropriate or excessive Personal Usage.

c) For Personal Use to continue it must:

- **be minimal and take place either during appropriate rest breaks or substantially out of normal working hours;**
- **not interfere with business or office commitments; and**
- **not commit Kraft Heinz to, or otherwise incur for Kraft Heinz, any costs, expense or expenditure.**

d) The use of webmail sites (such as Hotmail or Gmail) and online file sharing sites (such as Dropbox or GoogleDocs) to send or receive business related information is forbidden unless there is a genuine business justification for doing so and the site in question has been approved by the Data Privacy team.

11.13. Handling Customer Contact Details

a) You must either not leave any hard copy address books or other documents or devices containing business contacts unattended.

b) If you store business contacts electronically, you must store them in a secure area on Kraft Heinz's network.

12. Reporting Suspected Data Security Breaches

a) A data security breach may occur when a breach of data security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

b) This includes breaches that are the result of both accidental and deliberate causes.

c) Date security breaches may be a result of any of the following (this list is not exhaustive):

- Theft of data (including physical copies) or equipment (laptops, mobile phones, memory sticks, CD-ROMs, etc.) on which data is stored;
- User ignorance/lack of training;
- Unauthorised access/copying;
- Incorrect security classification/marking/labelling;
- Unsecured mode of transmission;
- Use of uncontrolled or unauthorised Media;
- Loss, or possible loss, of Media containing Personal Data;
- Loss, or possible loss, of devices or equipment;
- Loss or possible loss of backups;
- Inappropriate retention of Personal Data;
- Misdirection/misrouting of Personal Data;
- Incorrect method of disposal of Personal Data or Media containing Personal Data;
- Hacking/interception;
- Eavesdropping/espionage;
- Inappropriate release to the public domain;
- Access by unsupervised maintainers/contractors;
- Inappropriate access controls allowing unauthorised use by members of staff or others; or
- Information obtained by deceiving Kraft Heinz or Staff.

If you become aware of a Personal Data (or other) data security breach or suspect that one has occurred, you must immediately report this to the IT Service Desk and your line manager.

Data breaches may have to be reported to data protection authorities as little as 24 hours of discovery so it is vital that you report any actual or potential breach as soon as possible.

It is your responsibility to ensure that the potential data breaches report is received and that the Data Privacy Team are actively aware that it has been sent. Sending an email or leaving a voice message may be insufficient if you cannot be sure the recipient has picked up the message – always check.

When reporting a potential or actual data breaches you should try to provide as much information as possible (including but not limited to the following):

- What type of data was involved (whether Personal Data, Special Category Data or otherwise);
- When did the security breach happen;
- How did the breach occur (e.g. if data has been stolen or lost or whether unauthorised access is suspected);
- If the data has been damaged or corrupted, in what way has it been damaged or corrupted;
- How many individuals' Personal Data are likely to be affected by the breach;

- Who are the individuals whose Personal Data has been lost (i.e. are they are they Staff, customers, consumers or suppliers);
- Steps taken or to be taken to prevent further issues;
- Whether the breach is a repeat occurrence or if further Personal Data is being affected; and
- Any known contractual commitments given to third parties regarding the security of the Personal Data (e.g. to Kraft Heinz's customers).

You must then assist in stopping or mitigating the data security breach as instructed by the Data Privacy Team.

13. Ensuing Individuals Know How Their Personal Data Will Be Used by Kraft Heinz

In certain circumstances the express consent of individuals will be required.

Kraft Heinz has standard privacy statements and clauses which it has incorporated into its standard contract terms to ensure this requirement is met and to provide guidance to those who need to know when express consent should be obtained.

14. Ensuring That Personal Data Is Accurate and Kept Up to Date

Any inaccuracies in Personal Data held by Kraft Heinz should be corrected by Staff across all the relevant systems. Any updates or changes to information provided by an individual at any time should also be made on Kraft Heinz's records.

15. Individual Rights

Data Subjects must be informed of their right to access, correct, erase or restrict the processing of their collected Personal Data.

16. Requests for Access to Personal Data

If any member of Staff receives a request for information referencing any Data Protection Law they must contact the Data Privacy Team immediately, to ensure that request is properly dealt with within the prescribed time limits.

17. Data Privacy Impact Assessments

If you are establishing new processes, policies or procedures, embarking on a new project, considering new suppliers or purchasing new systems which involve handling or transferring large volumes of Personal Data or that could have a material impact on personal privacy or the security of Personal Data processed by or on behalf of Kraft Heinz, then you are responsible for ensuring that a DPIA is carried out.

DPIAs may also need to be undertaken in relation to outsourcing and procurement projects.

See here for details of Kraft Heinz's DPIA processes and procedures.

18. Securely Disposing of Personal Data

If Personal Data is no longer required, you must ensure that it is disposed of carefully and securely.

19. Training

You must attend all courses regarding the protection and handling of Personal Data which Kraft Heinz asks you to attend. These may include off site and e-learning courses.

20. Data Protection and Disciplinary Action

If any individual contravenes (or is suspected of having contravened) any aspect of this Policy, appropriate disciplinary action may be taken in accordance with the relevant disciplinary procedure.

Depending on the seriousness of the conduct, disciplinary action may include dismissal without notice.

Kraft Heinz also reserves the right to take such other action against an individual (including removing access to others' Personal Data or limiting Systems access) as may be appropriate in the circumstances.

If any individual has any doubts about whether they are processing Personal Data fairly and lawfully, they should contact the Data Privacy Team before carrying out any processing.

21. Policy Language

The language of this Policy is English and in the event of any conflict in meaning between the English language version and any translation of it, the English language meaning will prevail.

22. Monitoring and Review of This Policy

This Policy is reviewed by Kraft Heinz on a regular basis. You will be notified of changes to the Policy via Kraft Heinz's website.

Date of publication: 22 May 2018

Appendix 1A

Kraft Heinz Europe
Employing Companies

25th May 2018

BeneLux

H. J. Heinz Belgium SA

Heinz Finance (Luxembourg) SARL

France

H. J. Heinz France SAS

Germany

H. J. Heinz GmbH

Ireland

H. J. Heinz Company (Ireland)

Italy

Heinz Italia S.p.a.

Netherlands

H. J. Heinz Supply Chain Europe B. V.

H. J. Heinz Holding BV Manco Elst

H. J. Heinz European Holding BV

H. J. Heinz Nederland BV

Poland

H. J. Heinz Polska Sp. Z.o.o.

Pudliszki Sp. Z.o.o.

Spain

H. J. Heinz Foods Spain SL

H. J. Heinz Manufacturing Spain SL

United Kingdom

H. J. Heinz Foods UK Ltd (UK)

H. J. Heinz Manufacturing UK Ltd

Appendix 1B

Kraft Heinz Europe
Other current or former trading companies registered with Supervisory Authorities

25th May 2018

France

Heinz Frozen & Chilled Foods B.V.

Ireland

H.J. Heinz Manufacturing Ireland Ltd

Noble Insurance Limited

Italy

Heinz Produzioni Alimentari S.r.l.

Netherlands

H.J. Heinz B.V.

Koninklijke De Ruijter B.V.

United Kingdom

H.J. Heinz Trust Ltd

H.J. Heinz Pension Trust

H.J. Heinz Pension 2000 Trust

H.J. Heinz Frozen & Chilled Foods Ltd

Appendix 2

Types of Staff Personal Data Kraft Heinz may Process

Kraft Heinz may collect, store and process Staff Personal Data in respect of actual and potential Staff.

Staff Personal Data may include the following types of information and associated records, documents and copies:

- Personal contact details, including name, physical and email addresses and telephone numbers
- Biographical information, including date of birth and gender
- Family details, including marital status and dependents
- Next of kin details and emergency contact information
- Passports and visas
- Immigration status and right to work
- Job/role applications, including resumes, CVs, covering letters and associated documentation
- Academic, professional and other qualifications
- Driving licences and other license or authorisation documents
- National Insurance/national I.D number
- Employment records, including engagement dates and locations, training records, appraisals, career development and succession planning
- Bank details,
- Remuneration, including salary, bonus, pensions and other benefits (including Personal Data required to administer them such as details of persons nominated as potential beneficiaries)
- Attendance and performance records
- Systems activity data
- Telephone, video conference and similar call recordings (where made)
- Disciplinary and grievance information
- Photographs
- CCTV images
- Sound recordings
- **Special Category Data**
  We may only collect, store and use the following "Special Category Data" where we believe we have a legitimate business reason, and are legally permitted, to do so:
  - Information about race or ethnicity, religious beliefs and sexual orientation
  - Trade union membership
  - Information about health, including any medical condition and health and sickness records
  - Genetic information and biometric data.
  - Information about criminal convictions and offences

Not all of the types of Personal Data listed above may be collected or processed for all Staff.

Personal Data may be held before, during and after the period during which Staff are employed or engaged.

Members of Staff wishing to confirm which categories of their Personal Data Kraft Heinz holds should contact their usual HR team contact in the first instance.

Appendix 3

Processing of Staff Personal Data

Kraft Heinz may process Staff Personal Data for the following purposes:

- decisions about recruitment, appointment and promotion
- confirming information contained in job/role applications including in resumes, CVs, covering letters and associated documentation
- confirming immigration status, rights to work and rights of residency
- undertaking criminal records checks where permitted and considered necessary
- obtaining credit, conflict of interest, compliance and other checks, verifications and clearances
- performing reference checks and providing reference letters
- operation, administration and termination of contracts with, in respect of or relating to Staff
- Staff management including training, appraisals, performance evaluation, career development, promotions and succession planning
- provision, administration and review of salary, benefits, incentives, pensions and other remuneration including making taxation and other deductions we are required to make
- health and safety records and management
- equal opportunities monitoring
- complaint, grievance and disciplinary investigation, management, resolution and recording
- corporate and personal security (which may include use of CCTV and other visual or audio monitoring)
- operation of any ethics, compliance or whistleblowing hotlines which Kraft Heinz may run now or in the future
- in connection with any potential or actual corporate transaction or transfer of employment arising in relation to a business transfer or change of service provider in which case Personal Data may only be disclosed to the potential purchaser or investor and their advisors to the extent permitted by applicable law (such as the Acquired Rights Directive in Europe)
- conduct of Kraft Heinz's business and operations including provision of Staff information to customers, suppliers other third parties as reasonably required
- disclosures required in the connection with promoting or marketing of Kraft Heinz, its products or services by or to Staff
- compliance with applicable procedures, laws or regulations
- investigations to ensure compliance with or identify/confirm any potential breaches of any applicable policies, procedures, laws or regulations
- establishing, exercising or defending legal rights
- any other reasonable purposes in connection with an individual's employment or engagement by Kraft Heinz and the operation of Kraft Heinz's business;
- providing, managing, administering (including billing where required) services provided to Staff by third parties including but not limited to services in respect of mobile devices, company credit cards and company cars

- working with suppliers to whom Kraft Heinz has outsourced business or other services
- System operation and management
- processing necessary for the purposes of the legitimate interests pursued by Kraft Heinz

Appendix 4
Types of Third Party Personal Data Kraft Heinz may Process

Kraft Heinz may collect and process Third Party Personal Data which may include:

- Names, addresses, telephone numbers and other personal contact details;
- Consumer preferences;
- Consumer lifestyle Information;
- Direct marketing information;
- Website access and use data;
- Customer and Consumer IP addresses
- IT application access and use data;
- Health & safety data;
- Financial information including details of shareholdings, other forms of investment and the investors making them;
- Visitor logs for Kraft Heinz premises;
- CCTV images;
- Systems activity data and call recordings where made; and
- Sensitive Personal Data (principally health, genetic and biometric data) where permitted.

Appendix 5

Processing of Third Party Personal Data

Kraft Heinz may process Third Party Personal Data for or in connection with the following purposes:

- the proper conduct and development of Kraft Heinz's businesses and operations;
- research including consumer and market preferences to assist with the operation and development of Kraft Heinz's business;
- assisting with the development of existing and creation of new Kraft Heinz products and services;
- the manufacture of Kraft Heinz Products and supply of those products to Kraft Heinz customers;
- promotional and marketing activities (including running competitions and prize draws) in relation to Kraft Heinz's business and products;
- other disclosures required in the connection with promoting or marketing of Kraft Heinz, its products or services by or to Kraft Heinz Staff;
- financial and other forecasting and modelling;
- operation, maintenance and development of Kraft Heinz's Systems, networks and the equipment associated with or connecting to those systems and networks;
- development of Kraft Heinz's business through mergers, acquisitions, disposal and other corporate actions;
- dealing with actual and potential shareholders, investors and other stakeholders in Kraft Heinz's business;
- maintenance and protection of Kraft Heinz's physical and intellectual property and assets;
- protecting corporate and personal security (which may include use of CCTV and other visual or audio monitoring);
- recording, responding to, dealing with and resolving matters arising in respect of Kraft Heinz products or Staff;
- recording, responding to, dealing with and resolving actual or potential complaints from customers and consumers;
- investigations to ensure compliance with or identify/confirm any potential breaches of any applicable procedures, laws or regulations;
- establishing, exercising or defending legal rights;
- working with suppliers to whom Kraft Heinz has outsourced business or other services;
- in connection with business acquisition, disposal or reorganisations other than where information is exchanged in connection with a legal obligation as set out above.
- processing necessary for the purposes of other legitimate interests pursued by Kraft Heinz