KLP Data Protection Policies

Contents

Introduction

Kilkenny LEADER Partnership (KLP) takes seriously the need for data protection. The Company understands the importance of the necessity given the high volume of sensitive data retained by the company. This date is comprised of information on KLP's staff, board directors, members, participants on its various sub-committees, sub-contractors, project partners. This is in addition to the communities and clients with whom we work. KLP has therefore put in place detailed systems which aim to protect this data and assist the company to comply with the *General Data Protection Regulation* (GDPR) which came into force on the 25th May 2018.

All staff, board directors, sub-committee participants and sub-contractors of KLP are required to read the attached document, and adhere to the guidance provided within it. All sectors listed above are both data users and data subjects, and should therefore bear this in mind when reading this document. KLP staff should read this document in conjunction with their staff handbook.

KLP has appointed Bernie Thorpe as the company Data Protection Officer, but reminds all stakeholders that they have a part to play in ensuring that the company meets its GDPR requirements.

This document is a consolidation of KLP's data protection documents, with samples of logs, agreements etc. included in the appendix. This document will be reviewed, and amended, as the need arises, at least once a year.

Glossary

GDPR	General Data Protection Regulation, which became effective on the 25th of May 2018. This is an EU regulation, not just a national one.
DPC	Data Protection Commissioner.
DRCD	Department of Rural, Community and Development.
RDP	Rural Development Programme, also referred to as LEADER
Data Subject	the person whose data KLP is using or storing.
Data User	KLP and its staff.
CEO	Chief Executive Officer
ACEO	Assistant Chief Executive Officer
FC	Financial Coordinator
DPO	Data Protection Officer
DO	Development Officer
Ad	Administrator

Data protection policy

How KLP operates:

This covers all data subjects of the Company, including clients, employees, board directors, sub-committee participants, company members, subcontractors etc. KLP works with individuals, community groups, enterprises, families and a broad range of sectors of society to assist them to effect positive change to their individual lives and to generally improve the quality of life of the communities in Kilkenny. To enable KLP to bring about these changes, it is necessary that the Company gather information and analyse information and data. When you contact us we will regularly begin the process of gathering and recording information for the purpose of assisting you as an individual- or the community of interest, which may involve information that specific to you (e.g. addresses, phone numbers, etc.). However the information gathering and recording is enacted using a defined process, which allows you to decide what data of yours you are happy with us recording and how we use it. For that reason you may be asked to sign a data consent form.

Protecting your information:

KLP has always been conscious of how we store our client's data, however under a new data protection law, the European Union's *General Data Protection Regulation* (GDPR), which came into force on the 25th of May 2018, this duty to protect data needs to be more clearly documented. GDPR enhances your rights (as data subjects) over your personal data, and requires KLP to take extra steps to ensure that it is protected. We understand that data subjects are concerned about how their information will be stored and used, and ask that they trust us to do so, in a safe and secure manner.

What is Personal Data?

Personal Data is defined as any data which identifies the data subject or which can be used along with other information to identify them. This includes a variety of details, including your name, address, date of birth, *Personal Public Service* (PPS number) and other contact details.

What is Sensitive Data?

Sensitive data is described as information which individuals provide in order to help KLP design a development pathway or process to the individual's benefit. This can include details around their current circumstances, education, employment history, bank details, current enterprises, and any barriers that you have encountered in the past to prevent them from achieving their goals.

Why we collect clients information:

- To ensure that we are the service best suited to meet our clients' objectives.
- To prepare a plan to ensure that clients meet their goals, while addressing their challenges.
- To track the progress that we have made in achieving clients objectives.
- To work with clients in creating a progression plan and track their achievements.
- To identify 'what works well for both of parties' and how we can use this to improve our services.
- To assist clients in receiving grant aid, by providing the information required by funders, to ensure that they are eligible, and have all the required documentation for the application.

How we process your (the clients) information:

We process your personal data, of which there is a variety, in order to provide you with our services. Under the data protection law we are required to let you know that we need your agreement (consent) which is why you will be asked to sign a data consent form, or your personal action plan pack, depending on the service you are availing of. This allows us to process your personal and sensitive data and commence working on your behalf. As a result of this:

- Your personal data will only be provided to you alone.
- We keep your data for no longer than is necessary, based on the purposes for which we collected it, and in accordance with the contract requirements of our funders, as per our **Data Retention and Destruction Policy**.
- All files and data will be destroyed in a confidential manner.
- We may share you data with other service providers, when making appointments on your behalf with them, employers, trainers etc. You will be informed of this however in advance.
- In the case of LEADER RDP project promoters, your information will be shared with KLP's Evaluation Committee, and Board, as is a requirement under the programme, to allow them review your application and make decisions on it. Your DO will inform you of this process at application stage.
- KLP retains personal data for all Board directors, to enable it comply with company law, and contact directors to arrange Board, and sub-committee meetings.
- KLP retains personal data for all Board Evaluation Committee members, to facilitate their work in project evaluation: contacts, 'declarations of interest', etc..
- KLP retain a personal data for all company members, with their contact details to inform them of events, the company's AGM etc.
- KLP retains personal and sensitive data for all staff, in line with the employment Acts, to ensure payment of salaries, pensions and compliance with revenue payments.

Our role in protecting your information:

KLP is responsible for retaining your personal and sensitive data in a secure manner, both in 'soft copy': i.e. on computers/ laptop- or in traditional 'hard copy' (e.g. paper documents). We will retain your data carefully taking care to ensure its security and confidentiality is maintained at all times. All staff are aware of the need to protect client data, and in particular those who are in more open offices and public areas, where they are required to ensure that no data is left open on machines, or on desks for access by those entering the building, or indeed by another staff member who is not authorised to do so. KLP staff are required to shut down open screens on their laptop's/PC's when leaving their desk, and can only discuss client information with other staff members working on the same caseload. KLP staff across all programmes only have access to that data which is relevant to

their specific role, with the exception of Line Managers. In the case of Line Managers, staff may seek guidance on a specific client based issue, to their Line Manager. This is acceptable.

All paper data is stored in a locked filing cabinets when not in use, and on our secure databases. In order to protect your information we use security measures that comply with Irish law, including computer safeguards, and secure filing and buildings.

From time to time it may be necessary to check with you regarding the data we hold on you to ensure that it is up to date and correct. You should inform us if your information changes or you believe that we hold information on you which is incorrect, so that we can change it.

KLP also have a **Privacy Statement**, which is printed later in this document, and is also accessible on our website.

Your rights:

Under GDPR you have the right to request a copy of your personal and sensitive data from us, and if you so which ask that your data be deleted permanently.

You may have some queries or complaints in connection to our processing of your personal and sensitive data and should feel free to get in touch with our DPO at 056 77752111 or via email to bernie.thorpe@cklp.ie.

In the case of disputes, you should know you also have the right to lodge a complaint directly with KLP, in line with our **Complaints Policy**, outlined later in this document, or with the Data Protection Commission, if you are unhappy with our processing of your data. Details of this process can be obtained on www.dataprotection.ie or calling the Data Protection Commission on 1890 252 231.

Data Access Policy

Your entitlement to request your data held by KLP:

You have a right to request and be provided with a copy of your personal and sensitive data held by KLP in either paper or electronic format, hereafter referred to as data. This policy outlines how you can make this request.

How do I request a copy of my data?:

You can write, call or email KLP requesting a **Data Request Form** contained in Appendix 1 of this document**.** A copy of the data request form is also available to download from our website www.cklp.ie.

Phone: 056 7752111

Email: bernie.thorpe@cklp.ie

Writing: Bernie Thorpe, Kilkenny LEADER Partnership, 8 Patricks Court, Patrick St., Kilkenny.

You will also need to provide evidence of identification when you make the request, so that we can confirm we are not providing your data to anybody other than you. This can be in the form of a driving licence, passport or public service card.

You will receive a response from KLP within a month.

What information is needed to process the request?:

As stated above a completed Data Request Form, is required along with evidence of identification, as listed on the form. In order to process the request, KLP needs:

- A completed, signed and dated Data Request Form.
- A copy of your proof of identity and address should accompany the Data Request Form.
- The Data Request Form should be sent to the DPO, at the contact details listed above.
- If you have difficult downloading the Data Request Form from our website, contact us by phone or email and we will post or email one out to you.
- You will in the Data Request Form need to provide us with specific details around the information which you wish to access.

If you do not provide the required information to KLP, it may cause a delay and failure to supply may the required information mean that KLP will not be able to process the request.

What data or information can I request?:

All personal and sensitive data which KLP hold on you can be requested including:

- Why this data has been collected and stored?
- Those who have had access to this data, in KLP and third party if it applies.
- How the data has been stored?
- Any comments or expressions of opinions formed based on this data.

What happens once my request is in order?:

Once the completed form has been received by the DPO the following steps will be taken:

- Proof of identity will be checked.
- The data will then be requested from the relevant staff members within the company, and a thorough data search will be carried out.
- If the request is complex and detailed, you will be contacted within a month, by the DPO notifying you of this and giving you the time line for completion, not to exceed three months for the supply of the data.
- Data will be supplied to the requestor, in hard copy format
- The requestor will be asked to confirm what actions they wish to take with regard to the data.

What actions can I request be taken with my data?:

Once you have had access to your data you can request the following:

- You can request that some or part of your data is 'blocked', at which point there will be a flag placed on the specific data, restricting access to it, or preventing processing of the data for certain purposes, which you have requested.
- Where elements of the data being held on you, have been received it from a third party as a result of a referral etc., or a change in the data has arisen due to passage of time, you can request that this data is corrected.
- You can also request that your data is deleted/ erased from KLP systems in hard copy and electronic format.
- You can request not to receive any marketing, or promotional material from KLP such as newsletters, events or training taking place.

Privacy Statement

This privacy notice provides information about the ways in which the office of the Data Protection Commissioner (the DPC) collects, stores, shares or keeps personal information provided by our customers. This policy is also posted on KLP's website.

How KLP operates:

KLP works with individuals, community groups, enterprises, families and a broad range of sectors of society to assist them to bring about with our guidance positive change to their lives and communities in Kilkenny. In order for KLP to achieve this along with its clients, we need to gather information, will help identify your current circumstances, and where you would like to see yourself in the future. When you contact us we aim to work with you, assisting you to enhance your skills, capabilities and goals, via a route which is agreed with you and best suits your needs.

Protecting your information:

KLP have always been conscious of how we store our client's data both personal and sensitive (here after referred to as 'data'), however under a new data protection requirement, the *General Data Protection Regulation* (GDPR) which came into force on the 25th of May 2018, this needs to be more clearly documented. GDPR enhances your rights over your personal data, and requires KLP to take extra steps to ensure that it is protected. We understand that you are concerned about how your information will be stored and used, and ask that you trust us to do so.

What is Personal Data?:

Personal Data is defined as any data which identifies you or which can be used along with other information to identify you. This includes a variety of details, including your name, address, date of birth, PPS No., and contact details.

What is Sensitive Data?:

Sensitive data is personal data which provides more detailed information on you. It includes details around your current circumstances, education, employment history, bank details, current enterprises, and any barriers that you have encountered in the past to prevent you from achieving your goals. It would also include a person's:

(a) racial or ethnic origin of the person;

(b) political opinions;

(c) religious beliefs or other beliefs of a similar nature;

(d) membership of a trade union;

(e) physical or mental health or condition;

(f) sexual life;

(g) commission or alleged commission by the person of any offence; or

(h) any proceedings for any offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings.

Using the KLP website:

Our website (www.cklp.ie) has introduced cookies with effect from the 25th May 2018. The purpose of the cookies is solely to assist us in redesigning our website ensuring that we provide relevant information in an easily accessible format. Please see our **Cookie Policy,** which is included below after this Privacy Statement**.** KLP's website does not collect any personal data, apart from information that you volunteer (for example, when filling a form) and your IP address. Any information you provide in this way is used only for the purpose for which you provide it.

Any personal information you provide will be used only for the purpose supplied. We will neither make attempts to identify individual visitors, nor associate the technical details listed above with any individual. It is our policy never to disclose such technical information in respect of individual website visitors to any third party unless obliged to disclose such information by a rule of law. The technical information will be used only for statistical and other administrative purposes.

Search engine:

The search facility on our website is an internal search function and only returns information that appears on the website.

Calling our Office:

KLP does not collect Calling Landline Identification (CIL) or any other information on the origins of a call. We do not record or retain phone conversations.

CCTV:

KLP does not have CCTV in any of its offices; however there is a CCTV recording system in the Company's Childcare Facility- Deenside Early Years. This is designed for use of ensuring the safety of the children and staff using the facility. KLP have a separate CCTV policy for Deenside Early Years in its suite of Data Protection Policies.

Emailing:

Any emails sent to us are recorded and forwarded to the relevant section. The sender's email address will remain visible to all staff tasked with dealing with the query. Please be aware that it is the sender's responsibility to ensure that the content of their emails is within the bounds of the law. Unsolicited material of a criminal nature will be reported to the relevant authorities and blocked.

For our part KLP staff when sending group emails will use the 'blind carbon copy' (bcc) function rather than the 'carbon copy' (cc) function, thus ensuring that group members email addresses are not accessible to anybody other than the sender and the receiver.

KLP do not specifically use the internet to market events, but do from time to time inform clients/Board member/ community groups etc. of events which are of interest to them, and in this case will bcc group emails to them, or web texts.

However, if at any time a recipient decides they do not want to receive a communication of this type they have only to respond asking future communications to stop and KLP will remove them from the mailing list. All staff have been instructed that if this happens they are to go immediately to the mailing list and any other lists which may have the individual/community groups contact details on it and flag as such. They should also inform the DPO of this, so that request can be logged.

Your information and data consent:

When you first call to our offices, or make an application for funding, in order to assist or direct you to the best of our ability, it will likely be necessary even at first contact, to take basic information from you, some of which may be personal data. If you subsequently meet a Development Officer (DO), on your proposal/ application, they too may gather some personal or sensitive information from you. At that point you will be asked to sign a data consent form. These forms can vary depending on the programme, you are being assisted under. Data consent forms come as a requirement from KLP's funders, and are therefore specific to each programme. Thus there can be a slight variance in the wording, as a result of which if you move from getting support under one programme to another, you may be asked to sign a second data consent form.

The Data Consent allows us to use your data to assist you in accessing the service, while protecting your identity. KLP will store your data in hard copy in a secure place, and in soft copy on a fully encrypted device. Your data will not be released to a third party, without your direct permission, and only to assist in training programmes, employment or grants etc.

KLP will only use your information to contact you in relation to events, training and activities, which it judges suits your specific interests or needs. You can of course request that this does not happen, and your information will flagged as such. Should you at any stage receive communication from KLP which you feel you do not require, feel free to request us to stop these communications.

You are free to contact the offices of KLP to find out what data we have stored on you, and if you so wish ask that that information be erased or destroyed, as set out in our **Data Protection Policy** and **Data Access Policy,** also contained in this document.

KLP will destroy all data on individuals and community groups it has complied based on its **Data Retention and Destruction Policy**, also contained in this document.

Partners/Funders:

KLP is funded by a number of different state organisations, who from time to time ask for information as to how our programme is performing, for the majority of these programmes the information sent to them is anonymised. However those applying for grant aid under the LEADER Programme (RDP), should be aware, that the *Department of Community Rural and Development* (DRCD), its inspectors, and *Pobal* also have access to the information which is loaded on their website for processing and approve of funds. Information on this process will be provided to project promoters under LEADER/ RDP by their DO as part of the application process.

In the case of our accountants, and other suppliers, such as out IT consultants, who also have access to data in the course of their work with KLP, we will be putting in place a **Data Protection Agreement** (see Appendix 2 of this document) in our contracts to ensure your protection.

Publishing Data

KLP does gather information and publish identifiable 'case studies' in documents with a public or wide, if restricted circulation. In these cases the permission of the relevant person identifiable will be secured before publication.

The Company also gathers statistical information on the other projects and initiatives from individuals. Where these are not recognised case studies (as described above), all information gathered is anonymized or aggregated before publication and will not identify any individual or their personal and sensitive data.

Making a complaint to KLP:

When KLP receive a formal complaint, a file is generated. This will usually contain personal information about the complainant and any other individuals involved in the complaint. KLP will only collect personal information that is necessary to investigate the complaint. The Company has a **Complaints Policy** in this document, which outlines the process to be followed. A copy of the **Complaints Form** is in Appendix 4 of this document.

KLP will usually have to disclose the complainant's identity to whomever the case is against. We will try to facilitate a complainant who wishes to remain anonymous, but if a case proceeds it is generally inevitable that the identities of both parties are revealed. This is to ensure fairness in the legal process.

If sensitive personal data is collected for the purposes of a complaint, appropriate measures will be taken to ensure that it is safely processed.

The information contained in complaint files will be kept in line with our **Data Retention and Destruction Policy**. This means that information will be held for six years from the last date of action on the file. It will be kept in a secure environment and available only to those who need to access it.

When we take enforcement action, we may publish the identity of the defendant in our Annual Report or elsewhere. We will not identify the complainant, unless the information is already in the public domain.

Disclosure:

As far as possible, we will not disclose personal data without consent. However, when we investigate a complaint we may need to share personal information with the other parties concerned. We will consider any request for anonymity in respect of a case, but we cannot guarantee that it will be possible to enforce it. We will not disclose your personal data to third parties except in instances where an individual has consented to the disclosure, or we are obliged by law to disclose the data. Third parties to whom we may disclose information include organisations such as An Garda Síochána for investigation or legal purposes if so legally required.

Cookie Policy

County Kilkenny LEADER Partnership Clg. (KLP) reserves the right to amend this statement at any future date and will post any substantive changes here.

What is a cookie?

A cookie is a small piece of data that may be stored on your computer or mobile device. It allows a website "remember" your actions or preferences over a length of time. Some cookies can be read by the website on your subsequent visits. The information stored in a cookie may relate to your browsing habits on the webpage, or a unique identification number so that the website can 'remember' you on your return visit. Other cookies are deleted when you close your browser and only relate to the working of the website. Generally speaking, cookies do not contain personal information from which you can be identified, unless you have furnished such information to the website.

Cookies may be set in a number of places on this website:

- When you first visit this website, you will see a message informing you about the privacy statement. If you click the 'Hide this message' button, a Cookie will be set which records this action.

Most browsers allow you to turn off Cookies or to customise your settings for cookies. To find out how to do this, see the 'Help' menu on your browser. Please note that if you turn off cookies or change your settings, some features of this site may not work correctly.

Further information on cookies can be found at the following website:
http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

Links

From time to time the KLP website may contain links to other partner or stakeholder websites. *County Kilkenny LEADER Partnership Clg.* (KLP) is not responsible for these sites or for the privacy statements of other websites.

Photo and Images Policy

Why do we need this policy?

The purpose of this policy is to set out general rules about the capture and distribution of images, photographs videos etc., of all persons connected or interacting with KLP. This list includes but is not restricted to: clients, project promoters, Board members, Sub-Committee members, staff and children. The aim being to give staff, third party sub-contractors and the data subjects themselves, guidelines on the subject. It applies to activities on under taken by the company, including but not limited to, Board events, training events, information nights, site visits, staff events and one to one meeting be they in KLP offices or in an alternate venue based on the activity involved.

While children are covered in this policy, KLP also has a linked Childcare Facility, Deenside Early Years, which has its own specific set of Data Protection Policies, in addition to those contained in this policy.

"Image capture", "photography" and "videoing" refer to any kind of image capture, still or moving, obtained by any photographic device including still image cameras, video cameras, webcams and photographic enabled mobile telephones, and any other type of image capture device not specified here, whether digital or not, using technology existent at this time or in the future. The storage of such images includes film negative, film positive (e.g. transparencies and slides, movies, etc.), photographic paper, digital media, magnetic tape and any other kind of storage method able to be used for the storage of images, still or moving, available now or in the future.

This policy forms part of a suite of **KLP Data Protection Policies** and should be read as such. Children and young people, as well as adults have a right to privacy and therefore their consent should be sought in relation to use of personal data, including images. In the case of children (up to 18 years of age) parental or formal guardianship consent should be sought on foot of information provided on how and for what purpose images will be used.

KLP works with children, and young adults, via a number of its programmes and its linked company Deenside Early Years. It is important to highlight that KLP at all times, believes in safeguarding, children and vulnerable adults when in our care, or whom we may have course to interact with during the course of our work.

General principles for KLP Staff

Every reasonable effort must be made to minimise risk of inappropriate capture and distribution of photos and images. This includes:

- securing written parental consent for the use of images of their children i.e. those persons under the age of 18.
- securing written consent for any individual or the individual members of a group where the photo taken allows them to be clearly identified, no matter how closely linked they are to KLP.
- do not use photographs of Board members, Sub-committee members, clients or staff (data subjects) who have left the company, or have little or no contact with the company, without previously having got their written consent.
- ensuring that children and staff are appropriately dressed

- ensuring that children's, young people and vulnerable adults names are not used alongside images in publically-available material
- not using an image of any child or adult who is subject to a court order;
- storing images securely and accessible only by those authorised to do so
- storing images securely (whether physical or digital) with appropriate access controls
- ensuring staff are appropriately informed about this policy

Safeguarding

There may be a risk to the welfare of children when individual children can be identified in photographs. For that reason, we have developed this policy to make every effort to minimise risk.

Where the capture or distribution of images of children raises a safeguarding concern, the ACEO must be contacted immediately. The ACEO will investigate the matter in conjunction with the DPO and they will take, appropriate action, based on the specific situation.

Data Protection Act

Photographs and video images of data subjects are classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such images for KLP's publicity purposes requires the written consent (Appendix 3.a *Data Subject Consent* or Appendix 3.b *Parental Consent Form*) of either the individual concerned or in the case of all young people under the age of 18, their legal guardians. In line with the Data Protection Act, everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside EU without adequate protection
- use this document in conjunction with all documents in this suite of policies.

Photography and image capture

Images of data subjects may be captured as part of the KLP's activities; these may include but are not restricted to:

- Recordings of clients for training purposes, e.g. Interview skills, or as a means of accessing achievement of a specific learning objective.
- Attendance and interaction at a group, training programme.
- Attendance and interaction at a publicly advertised information event.
- Attendance at the company's Board meetings, or Sub-Committee meetings, including the AGM.
- Site visits to project promotors, to provide evidence on the progress of the project, or the outcomes of the project, for funders.

- Staff training events and activities.

Images will only ever be taken using company equipment or by a designated external professional. Staff must not take or transmit any recording such events on any personal device. Staff should also be aware that taking photographs of colleagues using personal devices should only happen with the permission of that member of staff.

Images of data subjects must not be displayed on websites, in publications or in a public place without specific written consent. Where photographs are taken at an event attended by large crowds, this is regarded as a public area so it is not necessary to get permission of everyone in a crowd shot.

All media permissions must be kept on file for verification prior to posting an image or for inspection should any issues arise. A spread sheet will be retained on the central server, which will list those who have given permission for their image to be used, the context in which it can be used and the duration (appendix 3.c Register of Data Consent for images). Staff and Board members etc. will be asked to sign these consents as a matter of course, to avoid having to request completion on a regular bases (appendix 3.a Data Subject Consent Form).

Photography and image capture by parents

As a general rule no parent or visitor is permitted to use a camera (including a mobile phone's camera facility) whilst visting or attending Deenside Early Years. However, the Data Protection Act does not apply to photographs or films taken for personal use by family and permitted friends. Please refer to Deenside Early Years Social Media Policy regarding usage of images, on Social Media etc.

Exceptions to this rule are therefore made for some specific events such as plays, recitals, concerts, sporting events, open days or other promotional events. We strongly advise parents against the publication of any such photographs on the internet (e.g. on social media), where another child (not their own) can be recognised- and we will request parents to remove any such material if we deem it illegal, harmful or inappropriate in any way.

Where appropriate, our policy regarding this matter should be explained clearly to parents by a member of staff before difficult situations arise.

Publicity

KLP needs and indeed welcomes publicity, on what the company does and how it can impact on those who live in the county of Kilkenny. This promotion can be supported by utilising interesting photos or videos, displaying the type of work undertaken, the achievements made and the final impact of the project funded. It is also a requirement of a number of the funders of the programmes delivered by KLP that evidence of activities and funding spend is required via site visits and photographs.

Making use of photographs for publicity materials and to promote the KLP in the press can support staff in their work and help funders, project partners, clients and the local community understand and celebrate the company's progress and impact on the county. However, photographs must be

used in a responsible way. KLP needs to respect the rights of privacy and be aware of potential child/ vulnerable protection issues.

Monitoring

It is the responsibility of all KLP staff to support and monitor this policy. Any concerns should be brought to the attention of the DPO.

Mobile Phone Policy.

Purpose

The purpose of this Policy is to set out KLP's policy in relation to the issuing, usage and payment for mobile phones. The following conditions apply to each staff member with a Company mobile communications device regardless of time of issue of the device. Usage of a Company mobile device implies acceptance to the terms of the policy.

It is KLP's policy to provide mobile devices to employees where contact with them cannot always be made by a landline and where contact would be necessary in the course of their duties. Employees should therefore carry their device at all times when working- and the de fault position should also be that the phone be 'on'; to receive messages and calls. However, depending on the work situation- meetings, site visits, etc. and the level of connection appropriate in the circumstances, phone may be on silent, 'airplane mode' or- if required for safety or regulatory reasons of the venue concerned, be switched off for that period.

Definitions:

Device

For the purpose of this policy document, the term "Device" should generally be read to include mobile phones of any type provided by KLP

User

"User" is defined as an employee who has responsibility for a mobile phone/ communications/ data device.

Provision of Mobile Phones.

KLP mobile phones and data cards are allocated by the FC on receipt of a request duly authorised by the CEO or ACEO. Such requests must be based on a "business need", i.e.:

- Employees agree with the FC/Line Manager that they must be contactable at all times during working hours (or outside working hours if applicable).
- Employees whose duties require them to be away from their main office/base on a regular basis.
- Employees who are required to be contactable outside normal working hours, e.g. employees on-call and/or those who are required to take action in the event of an emergency.

The purchase a mobile device is at the sole discretion of the CEO/ACEO. Mobile devices must be ordered/purchased through the FC, this approval is done via email between them and the CEO/ACEO.

In the event that a mobile device is procured without prior proper authorisation, the staff member who purchased the device shall be personally responsible for all costs incurred in the purchase, rental, calls/data and any other add-on expenses that may have been incurred.

The standard issue mobile device will constitute a basic mobile phone device with voice and SMS text capabilities. Approval for devices with above standard specification will be at the discretion of FC, in consultation with the CEO/ACEO, based on the specific Users need, to carry out their duties.

Phone upgrade models will be assigned based on business needs/requirements only, and not on a staff preference basis.

Using Mobile Phones requires care and vigilance on behalf of Users. KLP staff using mobile phones must take steps to ensure the security of the data held on these devices. The mobile phone should only be used for ethical and lawful purposes. Accessing of any unlicensed or illicit material is forbidden.

Internet access on mobile devices will only be provided where there is a particular business requirement for it, with the approval of the CEO/ACEO. Network Service Providers will be instructed to bar such access by default. Email/Internet facilities on the device must only be used in accordance with KLP acceptable usage policy. Any security applications provided must be approved by KLP or its ICT advisors.

PIN/Passwords for mobile phones must be kept confidential at all times and must not be shared with anyone including family members.

All mobile phones remain the property of KLP at all times. All KLP data held on portable devices is regarded as KLP property, and may be subject to monitoring and auditing, should concerns arise.

All personal data and use of portable devices for personal use is uncontrolled by KLP. Any personal data stored on the device is the responsibility of the User and no responsibility can be taken by KLP for the security of this personal information. The User is responsible for all personal data held on the device.

Any mobile phone used in a public place (e.g. on a train or at an airport) are to be positioned so that it is not overlooked (shoulder surfing).

Security settings and software (e.g. profile managers, antivirus, firewalls, encryption etc.) on portable devices must not be interfered with, and attempts to bypass security controls such as jail breaking must not be performed.

Use of Mobile Devices

All mobile devices remain the property of KLP. Users must not use the SIM provided for use in a KLP issued device in any other device without the express authority of the relevant CEO/ACEO and in accordance with all other terms of this policy. Service Providers must provide a list of devices including their IMEI number to the Company on request and at regular intervals as provided for elsewhere in this policy document. It is the responsibility of each employee who is issued with a Company mobile device to:

- Ensure that the device is used only by the person to whom it has been issued, and to take whatever measures that may be necessary to prevent unauthorised use;
- Ensure that the device is used as an effective communications tool for work purposes. Calls should be effective and short. Excessive use of phones to the detriment of performance of the users duties is forbidden.
- Safeguard the device and associated documentation from damage or loss. Never leave the device unattended. Set the PIN code to ensure the security of the SIM card. Take appropriate measures when using a data card in order to prevent unauthorised access to the KLP network.
- Comply with Data Protection obligations and report any lost, stolen or damaged mobile device to the DPO at the earliest opportunity so that a remote wipe of data may be carried out.
- Familiarise themselves and comply with legislative requirements regarding the use of mobile devices. KLP does not accept liability for any penalty incurred by an employee who breaches the law with regard to the use of mobile devices.

The CEO or ACEO at his/her discretion may withdraw the use of an official mobile phone from any member of staff.

Mobile phones are supplied for official use, i.e. as a work tool. Users are permitted to use the device for non-work purposes only where such use does not impact on the performance of the employees duties and provided that any expenditure incurred in excess of the monthly fixed tariff rate must be reimbursed to the Company including the V.A.T. element. It is the responsibility of the FC, to review monthly bills, identify non-work / excess expenditure, and ensure the User is informed, following which an a plan for the repayment of same including VAT will be put in place. Summary reports of usage will be reviewed on an ongoing basis by FC and other authorised entities e.g. Audit, Finance, inspectors etc. to ensure compliance with this requirement.

Users should use the Company mobile device in conjunction with available internal and external landline phones and all other communications technologies provided in a manner which best achieves economical and practical effect, and are required to ensure that best value for money is achieved for KLP at all times.

For Users on fixed monthly voice tariffs, it is worth noting that it may be more cost effective for the User to dial local landlines, national landlines and national mobile numbers using the mobile device compared to using a landline.

The following restrictions must be enforced on all mobile phones and cellular devices that store or access KLP information:

- Access to KLP data must only be granted following appropriate authentication.
- Password complexity must be enforced on devices.
- Devices must lock after a number of minutes of inactivity.
- Remote wipe capability must be enabled to securely erase data on a lost/stolen device.
- All sensitive data must be encrypted on the device. No KLP data may be stored on a portable device in a clear text format.
- Where possible, antivirus software must be installed and configured to actively scan files on access.

- All transmission of KLP data must be encrypted.

Service Restrictions

Mobile devices are issued for the purpose of work related communication. In order to reduce the overall operating cost, certain restrictions will be applied as default.

The restrictions shall include:

- Directory Enquiry Numbers
- Premium Rate Numbers
- Dialing International Numbers unless work related
- Roaming Access While Abroad unless on company business.
- Sending of MMS messages (save where specifically requested and approved by SMT member for emergency services, cost recovery or enforcement inspection records)

Safety

Driving.

In the interests of staff safety and the safety of other road Users, KLP expressly prohibits the use of mobile phones and hands free systems while driving**.** Staff members must either:

- Park their vehicle safely before they take or make a call or,
- Utilise the divert function available on the phone.

Use of Devices while at work, or on KLP controlled sites

Employees must not use devices in any location or manner where it results in an increased safety risk. Such forbidden use includes, but is not limited to, the following:

- Internet access or SMS messaging while moving or stationary in close proximity to traffic.
- While operating plant or machinery.
- Where such use is likely to distract the User in a dangerous environment, or impact on ability to hear and/or discern warning signals from safety equipment or other persons.
- Use for internet or SMS messaging, where such use might impact on the User's perception of visible hazards when in motion.
- Where a person is in control of any works or site, having carried out an appropriate risk assessment, deems it unsafe to use a device (s)he may direct any member of staff to refrain from any such use and the member of staff shall comply with such direction.

Replacement/Repair/Care of Mobile Phones

It is advised that mobile phones be kept in a safe place at all times and protected from theft.

In the event of loss/theft of a mobile phone, the Service Providers and the DPO should be notified immediately by the holder of the phone and the number suspended to prevent fraudulent use of the phone. KLP has engaged a Mobile Device Management (MDM) Contractor (*Three*™) for any or all of the devices covered by this policy, the User shall also notify the MDM contractor of any loss or theft to allow the device to be tracked, locked and/or wiped of data as appropriate.

Approval in writing for the replacement of stolen/damaged mobile phones should be sought from the CEO/ACEO and forwarded to FC to procure. This may include a contribution from the staff member, who lost the phone depending on the replacement cost of the new phone; this decision will be at the discretion of the CEO/ACEO based on a consideration of the circumstances of the loss or damage.

Employees need to remember the following:

- Never leave mobile phones unattended and always lock them away when not in use.
- Do not leave any your mobile phone on your desk overnight; secure it in a locked drawer.
- Do not leave any mobile phones visible in an unattended vehicle.
- To prevent physical damage and loss of assets, wherever possible, remove all portable and mobile media from vehicles when they are left unattended. If this is not possible, they have to be securely locked away in a place where they are not visible.

Where an employee has received an upgrade or replacement device, (s)he must return the device being taken out of service to DPO within three weeks of receipt of the replacement.

It is proposed that contracts for the provision of standard phone handsets shall be on the basis where the tariff does not provide for subsidised asset replacement. In this case any replacements or upgrades shall be priced at the SIM free price as may be agreed with the Service Provider on a monthly basis.

Contracts for the provision of Smart phones shall be on the basis that an agreed maximum percentage of the phones may be upgraded during the currency of the relevant framework under a subsidised asset pricing and thereafter all smartphones shall be paid for as SIM free. For this reason, all upgrades must be on the basis of business need. Where the reason for upgrade results from carelessness on the part of the User, the Company reserves the right to recover some part or the upgrade cost from the User.

Staff Employment Exit

All devices are to be returned to the FC upon leaving employment with the Company.

Where a FC or CEO/ACEO is exiting employment with the Company (s)he shall make arrangements for the transfer of all accounts for which (s)he is responsible to the incoming officer, or another responsible member of the Company staff.

Disciplinary Procedure

Any employee found to be in breach of this policy may be subject to disciplinary action in accordance with the Company's disciplinary procedures. The CEO/ACEO department reserves the right to have a mobile service withdrawn at any stage.

Monitoring and Expenditure Control

1. KLP's policy is to procure Mobile Telephony Solutions under the public sector Mobile Voice and Data Services Framework
2. Each Mobile User, CEO/ACEO and FC is responsible for ensuring that the connection(s) is placed on the most cost effective tariff.
3. The attached Appendix 4.1 table sets out the responsibilities of each of the stakeholders.

4. The Company proposes to maximise the number of device connections that are charged on a fixed tariff. As all devices are on a fixed tariff and where no additional usage charges are incurred in any billing period, the account for such connection shall be deemed to be automatically verified for the said period and no further verification shall be required.
5. Service providers can now provide detailed statements for all users.
6. The following monitoring system will be put in place to support the stakeholder responsibilities:
    - **Financial Coordinator (FC):** The FC will examine summary and spend summaries monthly and identify usage levels for further examination with the user and line manager. Where summary reports show excessive usage for any user, the FC will identify the issue and bring it to the users attention. The FC may also make direct contact with the line manager for examination and action.
    - **Financial Coordinator:** The FC is to receive a monthly "Exceptions Report" from the Service Provider(s) regarding any User accounts within the team that are showing exceedances (see Appendix 3). It is the responsibility of the Financial Coordinator to review the Exceptions Report and take action as appropriate with regard to ensuring cost effectiveness and value for money for the Company.

Usage types (e.g. Premium calls, Premium texts, Roaming / International Calls, Data etc.) will be monitored on an ongoing basis. Non work-related expenditure is the responsibility of the User. Such expenditure shall be recoupable from the User, based on agreement with the Line Manager.

Spam texts are unsolicited texts sent to a User without his/her permission. Such texts are often sent on a scheduled basis and some such texts attract a premium text rate. Users and FC should be vigilant and if spam texts are being received, the User is requested to text STOP in response to the text.

KLP will continue to review mobile phone expenditure on an ongoing basis and will arrange to take any corrective action deemed necessary to ensure that value for money is being obtained for the Company. Financial Sub-Committee will be responsible for the monitoring, oversight and verification of spend.

Mobile Device Management

Billing Queries

In the case of billing queries, including incorrect tariffs and services that are available when they should be barred (or vice versa), Users shall in the first instance clarify the correct scenario with the FC and then note the issue to be resolved; this may then be forwarded to Corporate Affairs (Service Provider) by Email for resolution with the Service Providers contact person. It is proposed that the Service Provider should have a named individual and substitute assigned to manage the financial and contractual issues for the service.

Technical issues relating to levels of service, performance of handsets and repairs

It is proposed that the Service Provider shall have a dedicated helpline for technical support which may be contacted by individual Users to resolve any issues. Where the issue can only be resolved by repair of the device, the Service Provider shall issue a temporary replacement and recover the

device for repair. Where the device must be replaced, a report from the technical support/repair personnel shall be attached to the request for upgrade. In the case where there is a cost attached the user must seek prior approval form the FC, with the aid of a written quote (typically email) prior to progressing this action.

Externally sourced Mobile Device Management

Where the Company elects to engage a Service Provider for Mobile Device Management, such service may provide, inter alia, for:

- Security of Devices and Connections.
- Control of apps and other software on devices.
- Restrictions and other usage policy controls.
- Wiping of all data from mobile devices.
- Tracking the location of missing or stolen mobile devices.
- Monitoring device usage.
- Monitoring device internet and social media usage

IT and Security Policy

To be inserted

Note Data Retention Policy Appendix and table still need to be completed.

Data Retention and Disposal Policy

Introduction

The aim of this policy is to set out the data retention times and disposal methods for documentation and data held by KLP.

KLP keep a wide range of data, the retention guidelines for programme related data is set by the programme funders. A schedule listing the data retention times lines for all data, will be complied and included in the appendix of this document, once full confirmation is received from all funders as to the retention requirements.

What documents and data are we referring to?

In the case of KLP the data referred to is broad and varied but includes:

- All staff application records and CV's etc.
- All staff files including, pension details, holiday, sick pay and Toil records.
- All staff payments, including salaries, travel expenses, etc.
- All staff register of interests, and conflict of interest declaration forms
- All Board directors contact details,
- All Board directors register of interests, conflict of interest declaration forms and B2's for CRO.
- All KLP members, contact details
- The Evaluation Sub-Committee contact details
- The Evaluation Sub-Committee register of interests and conflict of interest declarations.
- All suppliers contact details, tax references, bank accounts and payment records.
- All contractors, tenders, contact details, bank accounts, tax references, copy insurances, contracts and payments across all programmes.
- All images will take by the company staff or professionals on their behalf.
- All RSS participant data, including, address, bank details, herd number, dependant details, work records, contracts payslips and payments details.
- All RSS sponsor communities, contact details, application forms, contracts and work plans
- All TUS participants data, including, address, back details, dependant details, work records, contracts, payslips and payment details.
- All TUS sponsor communities, contact details, application forms, contracts and work plans

- All SICAP clients, be they individual or communities, personal action plan or community action plan, containing details regarding the, name, address, personal details, education, employment records and progression.
- All SICAP clients/community payments.
- All RDP project promoters, bank details, accounts, business plans, contact details, payments, etc. all required to form part of a EOI or project application
- All Deenside Early Years data will be covered specifically by the Deenside Early Years data retention policy, with the exception of staff details.
- All National Walks Scheme participants, contact details, bank details, contracts and payments.
- All Housing Aid clients, contact details, invoices, job cards, and payments.
- All Newstart clients, contact details, details regarding education, employment and progression.
- All Primary Health care, contact details, training records, medical records, bank details and payments.
- And any other projects or programmes, being delivered by KLP.

Retention Period

KLP must comply with the provisions of the General Data Protection Regulation and the Data Protection Act 2018. This legislation sets out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it is obtained.

This requirement places a responsibility on KLP to be clear about the length of time personal data will be kept and the reasons why this information is being retained. To comply with this rule KLP must have a policy on retention periods for personal data retained. This policy is required to include defined detention periods for records and systematic disposal of records within a reasonable time period after the retention period expires. Retention periods are set by the legal requirements as in state law but also by the various programmes funders, and in some case the EU as a funder.

KLP is committed to effect data management, retention and disposal to ensure that:

- Meets the legal requirements in terms of retention periods
- Maximises the use of space
- Securely destroys outdated data.

The data retained can be split into different categories:

- Legal and Audit; CRO information, Revenue and audits accounts.
- Staff records
- Board and KLP membership records
- Project files and client data related to specific programmes
- Financial; KLP's financial records, payments, bank statements and reconciliations.
- Publications and promotional materials.

Deciding on the retention period

The retention period will be determined by the purpose of the data, the value of the data, and the relevant statutory requirements, regulations and policies; for example financial records, have a fixed retention period.

While in other cases as stated earlier the may not be legal requirements, but contractual obligations, which will affect the decision on the retention period.

In addition in exceptional circumstances the administrative and operational needs of the service may deem it appropriate to retain certain records for longer than the statutory retention period, but in such cases the rationale for this must be clearly recorded.

Implementing this policy

All records which have reached their retention period should be reviewed under the following criteria:

- Recommended retention period should be calculated from the end of the calendar month following the last entry or file closing.
- A review of all documents held will be carried out annual and from that a list of data to be disposed of will be identified.
- Line Managers must ensure the systematic disposal of all data within a reasonable period after their retention period expires.
- It is vital that the process of record disposal safeguards and maintains the confidentiality of the records. Where there are significant volumes of hard copy data for disposal an external approved company will be contracted in to dispose of the data. It is up to the Line Managers to satisfy themselves that the methods used provide adequate safeguards against accidental loss or disclosure of records.
- A register of records destroyed will be held by the DPO (See Appendix)
- Only those documents containing confidential information should be disposed of in this way, all other documents, should disposed of using recycling options for paper disposal.

How will data be destroyed and when?

Different data will be retained and destroyed in different ways, see our **IT Security Policy** and **Mobile Phone Policy** both in this document, regarding the disposing of the device, its hardware and the contents of same if the device becomes obsolete or needs to be replaced.

Corporate records

These records are specifically related to

Record	Retention Period	Final action
Board meetings Agendas and Minutes	7 years hard copy	Archive
Declaration of interests and conflict of interest forms	15 years hard copy	Destroy as confidential data

Ethics in public Office records	15 years hard copy access only by CEO	Destroy as confidential data.
Complaint files, FOI requests, Data Protection requests, **Etc.**	7 years hard copy	Destroy as confidential data.

Operational records

This data is data specifically relating to programmes being delivered by KLP, and therefore the retention period is dictated by the funders.

Record	Retention Period	Final Action
Contracts with Funders		
Complaints	5 years hard copy or long if required by a specific programme.	Destroy as confidential data
Correspondence	5 years hard copy or long if required by a specific programme.	Destroy as confidential data
Inspection reports/audits	10 years hard copy or long if required by a specific programme.	Destroy as confidential data
Files which were investigated	7 years hard copy or long if required by a specific programme.	Destroy as confidential data
Staff time sheets	7 years hard copy or long if required by a specific programme.	Destroy as confidential data
Staff travel expenses	Depending on the specific programme worked on see the programme section.	Destroy as confidential data
Staff diaries, not supplied by KLP	Disposed of at the end of the calendar year	Destroy as confidential data
Board Policies		
Outdoor Tourism files		Destroy as confidential data
LCDP Programme files		Destroy as confidential data

SICAP 2015-2017 Programme files.		Destroy as confidential data
SICAP 2018-2022 Programme files.		Destroy as confidential data
RDP 2007-2013 Programme files		Destroy as confidential data
RDP 2014-2020 Programme Files		Destroy as confidential data
All Programme Circulars	Indefinitely	
RSS Programme Files		Destroy as confidential data
TUS Programme Files		Destroy as confidential data
Housing Aid Programme Files		Destroy as confidential data
National Walks Scheme Programme Files		Destroy as confidential data
RRO Programme Files.		Destroy as confidential data
SCEN Programme Files		Destroy as confidential data
Newstart Programme Files.		Destroy as confidential data

Financial Records

Under Section 886 of the Direct Tax Act the Revenue Commissioners require that records are retained for a minimum period of six years, after the completion of the transaction, acts or operations to which they relate. This applied to both hard and soft copy data. It is the original files that they will require to review if an investigation is required.

As a large number of KLP Financial records relate to programmes listed above, the expenditure on those programmes will be required to be retained based on the specific programme needs, which will usually be longer than the six years required by revenue.

Record	Retention Period	Final Action
Tax Clearance Certificates		
Accounts Payable.		
Bank Statements		
Bank Reconciliations		
Cr. Card statements		
Lease Agreements		
Insurance Policies		
Vehicle Insurance Polices		
Asset Register		
Reports to Finance Sub-Committee		
Annual Accounts		
Cancelled cheques		
Purchase orders		
Tender reports, RFT and full process.		
Staff Records		
Authorisation to deduct from pay		
Taxation records P'60's etc.		
Bank Mandates		
Staff pension files.		

Recruitment

The list for recruitment is specific to the appointment of an individual to KLP's Core team, those recruited under the TUS, and RSS programme, will have their data retained as per the guidelines for that specific programme.

Record	Retention Period	Final Action
Post advertisement		
CV's Received		
Score sheet from selection process		
Letter of appointments		
Staff contracts		
Garda Vetting		
Staff training records		

Incident Response Policy

Purpose of this Document:

The aim of this document is to outline the procedure to be followed in the event that KLP becomes aware of the loss of personal data. This includes the obligations under law, General Data Protection Regulation (GDPR), which came into force on the 25th of May 2018.

Rational:

The response to any breach of personal data (defined by the legislation) can have a serious impact on KLP's reputation and the extent to which the public perceives KLP as trustworthy.

The consequential impact on KLP's reputation and its standing could be serious. Therefore, exceptional care must be taken when responding to a data breach incident. GDPR requires mandatory breach notifications, within 72 hours, unless the data is anonymised or encrypted. This means that most data breaches must be reported to the Data Protection Commissioner.

This policy covers both personal and sensitive data held by KLP, both in paper and automated forms. All personal and sensitive data will be treated with equal care by KLP, and will be referred to in this policy as personal data, unless stated otherwise.

What constitutes a breach potential or actual?;

A breach is the a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data.
- Lack of secure password on pc's and applications
- Emailing a list of clients, members etc., to someone in error.
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data.
- Sending marketing information or other information to somebody who has already requested to be removed from the database/ circulation list.
- Not providing a unsubscribe or stop option for those being circulated re events or training.
- Staff members seeing information on each other eg. Salaries.
- Staff members not working with a particular client or department,
- viewing a client's details etc.

Actual, suspected or potential breaches should be reported immediately to the DPO. **It should be noted that any employee who becomes aware of a likely data breach and fails to notify the DPO will be subject to KLP's Disciplinary procedure.**

A team comprising the CEO, ACEO and DPO will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of the data lost and the number of Data Subjects impacted the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances KLP will inform the data subjects of the loss of their data and provide them with an assessment of risk to their privacy. KLP will make recommendations to the data subjects which may assist in minimising the risk to them. KLP will then implement changes to procedures, technologies or applications to prevent recurrence of the breach.

When will the office of the Data Protection Commissioner be informed?;

All incidents in which personal data has been put at risk will be reported to the Data Protection Commissioner within 72 hours.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

Data Loss logging:

All data breaches will be recorded in an **incident log** (Appendix 6) as required under GDPR. The Log will maintain a summary of the record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner on request.

Complaints Policy

Kilkenny LEADER Partnership KLP is committed to dealing effectively with any complaints you may have about our service.

If we have made a mistake, we will apologise and where possible try to put things right. We also aim to learn from our mistakes and use the information we gain to improve our services.

When to use this policy

When you complain to us, we will usually respond in the way we explain below.

Sometimes, you might be concerned about matters that are not decided by us. This will be reviewed by CEO or Sub Committee dependent on the individual concerned or the subject of the complaint and we will then advise you about how to make your concerns known. This policy should be viewed in conjunction with our **Incident Response Policy** should as any of the concerns raised be of a data protection nature, KLP will need to enact its Incident Response Policy and if necessary inform the Data Protection Commissioner.

All data obtained and procured as a part of any complaint investigation, will be managed in line with our **Data Protection Policy**, which is outlined earlier in this document.

Informal Resolution

If possible, we believe it is best to deal with things as soon as possible and in the most direct way. If you have a complaint, raise it with the person you are dealing with. He or she will try to resolve it for you there and then. However, they may need time to look into the issues. This process should be completed in *up to 5 working days.*

If there are any lessons to learn from addressing your complaint, the member of staff will draw them to our attention. If the member of staff can't help, they will explain why, and if you so choose, you can then ask for your complaint to be formally investigated.

How to complain formally?

You can make a complaint in any of the ways below:

- You can ask for a copy of our **Complaint Form** (Appendix 5) from the person with whom you are already in contact.
- You can get in touch with our office on 056 7752111 if you want to make your complaint over the phone.
- You can e mail us at info@cklp.ie

What should you include in your complaint?

Remember to state your name, address and telephone number (and email, if applicable) and whether you are acting on behalf of someone else

Briefly describe what your complaint is about stating relevant dates and times, if applicable List your specific concerns starting with the most important concern:

- Be clear about what you are hoping to achieve (for example an apology, explanation, etc.)
- State your preferred method of communication
-

It will assist the Complaints Officer if extra information and/or copies of relevant documents are attached to your complaint.

Dealing with a complaint

We will formally acknowledge your complaint within up to 5 working days and as part of that process we will:

- Let you know how we intend to deal with your complaint

- We will ask you to tell us how you would like us to communicate with you and establish whether you have any particular requirements, for example; if you have language difficulties.
- We will deal with your complaint in an open and honest way.
- We will make sure that your interactions with us in the future do not suffer because you have made a complaint.

If you are making a complaint on behalf of somebody else, we will need their agreement to you acting on their behalf and you will be required to demonstrate you have this permission.

Investigation

We will tell you who we have asked to investigate your complaint. If your complaint is straightforward, we will usually ask somebody from the KLP staff to look into it and respond to you. In some cases, if the complaint is serious, we may ask someone from our Board of Directors, to be part of the investigation, or part of the panel reviewing the findings of the investigation.

- We will set out to you our understanding of your complaint and ask you to confirm that we have the correct understanding of the issue. We will also ask you to tell us what outcome you are hoping for.
- The person responsible for investigating at your complaint will usually need to see the files we hold relevant to your complaint. If you don't want this to happen, it is important that you inform us of this. But the Company will reserve the right to make its own decision on that request.
- ~~If there is a simple solution to your problem, we may ask you if you are happy to accept this.~~
- We will aim to resolve concerns as quickly as possible and expect to deal with the vast majority within 30 working days.

If your complaint is more complex we will:

- let you know within the five days period why we think it may take longer to investigate
- tell you how long we expect it to take.
- give you regular updates very 20 working days on any progress made

The person who is investigating your concerns will aim first to establish the facts. The extent of this investigation will depend on how complex and how serious the issues you have raised are. In complex cases, we will draw up an investigation plan.

In some instances, we may ask to meet you to discuss your complaint. Occasionally, we might suggest mediation or another method to try to resolve disputes.

When investigating your complaint, we will look at relevant evidence. This could include files, notes of conversations, letters, emails or whatever may be relevant to your complaint.

If necessary, we will talk to the staff or others involved and look at our policies and any guidance.

Outcome

If we formally investigate your complaint, we will let you know what our decision using the channel of your preferred form of communication. This could be by letter or email, for example. If

necessary, we will produce a longer report. We will explain how and why we came to our conclusions.

If we find that we have made errors, we will tell you what and why it happened. If we find there is a fault in our systems or the way we do things, we will tell you what it is and how we plan to change things to stop it happening again.

If we believe that we have made mistakes, we will always apologise. If necessary in line with our **Incident Response Policy** if there has been a data breach, the Data Protection Commissioner will be informed.

Putting things right

If we didn't do something well, we will aim to put it right. If you have lost out as a result of a mistake on our part we will try to put you back in the position you would have been in if we had got it right.

What we expect from you

In times of trouble or distress, some people may act out of character. There may have been upsetting or distressing circumstances leading up to a complaint. We do not view behaviour as unacceptable just because someone is forceful or determined.

We believe that all complainants have the right to be heard, understood and respected.

However, we also consider that our staff have the same rights. We, therefore, expect you to be polite and courteous in your dealings with us. We will not tolerate aggressive or abusive behaviour, unreasonable demands or unreasonable persistence.

Lessons Learned

We take your complaints seriously and try to learn from any mistakes we have made. Our senior management team considers a summary of all complaints on a regular basis as well as details of any serious complaints.

Where there is a need for change, we will develop an action plan setting out what we will do; who will do it and when we plan to do it by. We will let you know when changes we have promised have been made.

Appendix

Appendix 1 Data Request Form

Data Request Form: Request for a copy of Personal Data

Important: In order for us to deal with your request efficiently a copy of your proof of identity (e.g. passport or driver's license) should accompany this Data Request Form. Please note that we have the right to require that you identify yourself before we will respond to any access request (see Note below).

Section A

Full Name…….

Postal address*

……

……

……

* Where you would like us to send you a copy of your Personal Data by post, a copy of your proof of address (e.g. utility bill) should accompany this Access Request Form.

Telephone/e-mail*

…… (include area code)

*You do not have to provide us with your telephone number and / or email address. It is advisable to supply a telephone number and / or email address in order to facilitate KLP contacting you so that any clarifications can efficiently be made where necessary in relation to your request.

Section B

I, ……..[insert name] wish to have access to Personal Data that I believe KLP retains on me as outlined below. (In order to assist us in efficiently dealing with your request, please include the name of service/services which KLP provide that you availed of or inquired about, an estimate of the year, any reference number or name on correspondence you may have received from us.)

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

Signed…….. Date……

Checklist: Have you:	Yes	No
1) attached a copy of proof of your identity?	☐	☐
2) attached a copy of proof of your address? (where you would like to send a copy of your Personal Data by post)?	☐	☐
3) signed and dated the Access Request Form?	☐	☐

Please note that we have the right to require that you identify yourself before we will respond to any access request.

Please return this form:

- to the Bernie Thorpe, Kilkenny LEADER Partnership, 8 Patricks Court, Patrick St., Kilkenny or
- by e-mail to bernie.thorpe@cklp.ie . If you make a request by email, the information requested will be provided to you in electronic form (where possible), unless you request otherwise.

Note: we require proof of the applicant's identity and address to ensure that the person making this access request is acting legitimately.

Appendix 2 Data Processing Agreement for Service Providers

Data Processing Agreement (DPA) for service providers

The parties:

(Insert name) , the processor having an address at **(Insert Address),** will hereafter be known as 'the Processor'.

Kilkenny LEADER Partnership Clg (KLP), the controller having an address at 8 Patricks Court, Patrick St., Kilkenny, will hereafter be known as 'the Controller'.

The Controller having complied and gathered personal sensitive data on individuals and companies (hereafter known as 'Data Subjects'), aims to safe guard that data and this agreement has been drafted to assist in that process.

Introduction

This agreement relates to the processing of personal data on behalf of Kilkenny LEADER Partnership by (Insert name) and is attached as an addendum to the **(Insert: Service Level Agreement, Contract etc)** in which the parties have agreed the terms for the Processors delivery of service to the Controller. "Personal Data" includes *"any information relating to an identified or identifiable natural person"* as defined in GPRP, article 4. The categories and types of data being processed by the Processor on behalf of the Controller are listed in Appendix A. The Processor only performs processing activities that are necessary and relevant to perform the services based on the task they have been appointed to do.

Legislation

The Data Processor Agreement (DPA) will ensure that the Processor complies with the applicable Data Protection and Privacy legislation, including in particular the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Instruction

The Data processor may only act and process Personal Data in accordance with the documented instruction from the Controller, unless required by law to action without such instruction. The instruction at the time of entering into this DPA is that the Processor may only process the Personal Data with the purpose of delivering the Main Service as described in the **(Insert: Service Level Agreement, Contract etc)**.

Subject to the terms of the DPA and with the agreement of both parties the Controller may issue additional instructions consistent with the terms of the DPA.

The Controller is responsible for ensuring that all individuals who provide written instructions consistent with the terms of this Agreement.

The processor shall refrain from making use of the personal data for any purpose other than as specified by the Controller. The Controller will inform the Processor of any such purposes which are not contemplated in this DPA.

All Personal data processed on behalf of the Controller shall remain the property of the Controller or the relevant Data Subjects.

The Processor will take no unilateral decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the data.

The Processors Obligations

The Processor and their employees shall treat all Personal Data as strictly confidential information; it shall not be copied, transferred or otherwise processed in conflict with the instruction, unless it is agreed in writing with the Controller. Personal Data will only be made available to enable the Processor to deliver the main agreement in line with the DPA.

The Processor shall implement the appropriate technical and organisational measures as set out in this DPA and in the Applicable Law, including in accordance with GDPR, article 32. The security measures are subject to technical progress and development. The Processor may update or modify the security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security.

The Processor will furnish the Controller promptly on request with details regarding the measures it has adopted to comply with its obligations under the DPA.

Transmission of Personal Data

The Processor may process Personal Data in Ireland, and the EU. If the Processor proposes to transfer personal data to a country outside of the EU it will need to provide such guarantees adequately levels of protection that satisfy this DPA and GDPR regulations. The Processor will not transfer personal data outside of the EU without meeting these requirements and having the approval of the Controller.

Engaging third parties or subcontractors

The Processor is authorised within the framework of the DPA to engage third parties, but they are required to seek approval from the Controller, as to the level of access being applied.

The Processor shall ensure that the third party will be obliged to agree in writing to the same duties that are agreed between the Controller and Processor.

Duty to Report Breaches

In the event of a security leak and or the leaking of data, the Processor shall, notify the Controller thereof with undue delay, after which the Controller shall determine whether or not to inform the Data Subjects, and enact the investigation and reporting of the breach in line with the KLP Incident

Response Policy. The Processer will ensure that the information furnished is complete, correct and accurate.

If required by law or regulation the Processor shall cooperate in notifying the relevant authorities and/or Data subjects. The Controller remains the responsible party or any statutory obligation thereof.

The duty to report includes any leak which occurred, including details such as:

- The cause of the leak
- The known and or anticipated consequences of the leak
- The solution
- The measures that have already been taken.

Security

The Processor will take adequate technical and organisational measures against loss or any form of unlawful processing in connection to the performance of processing personal data under this DPA.

The Processor does not guarantee that the security measures are effective under all circumstances. The Processor will ensure that the security measures are of a reasonable level, having regard to the state of art equipment, the sensitivity of the personal data and the costs related to the security measures.

The Controller will only make the personal data available to the Processor if it is assured that the necessary security measures have been taken. The Controller is responsible for ensuring compliance with the measures agreed by and between parties.

Data Subject requests

Where a Data subject submits a request to the Processor to inspect, improve, amend, change or protect their personal data, the Processor will inform the Controller, who will implement the KLP Data Access Policy, and issue a KLP Data Request Form. The Processor may inform the Data Subject of the action taken.

Non-Disclosure and Confidentiality

All personal data received by the Processor from the Controller or compiled by the Processor within the framework of this DPA is subject to a duty of confidentiality vis-à-vis third parties.

This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such information to third parties, where the furnishing of the information to third parties is reasonably necessary in view of the nature of the instructions and the implementation of this DPA, or if there is a legal obligation to make the information available to a third party.

Documentation of Compliance and Audit Rights

Upon request by the Controller, the Processor shall make available to the Controller all relevant information necessary to demonstrate compliance with this DPA, and shall allow for the reasonably

cooperation with audits, including inspections by the Controller or an auditor mandated by the Controller.

Such audits may only be undertaken when there are specific grounds for suspecting the misuse of personal data.

The Controller shall give notice of any audit or document inspection to be conducted and shall make reasonable efforts to avoid causing damage or disruption to the Processors premises, equipment and business in the course of such an audit or inspection. Any audit or document inspection shall be carried out with reasonable prior written notice of no less than 30 days and shall not be conducted more than once a year.

The findings in respect of the performed audit will be discussed and evaluated, by the Parties and where applicable, implemented accordingly as the case may be by one of the Parties or jointly by both Parties.

The cost of any other audit should be borne by the Controller.

The Controller may be requested to sign a non-disclosure agreement reasonably acceptable to the Processor before being furnished with the above.

Duration

This DPA is entered into for the duration set out in the **(Insert: Service Level Agreement, Contract etc)**.

The DPA may not be terminated in the interim.

The DPA can only be amended subject to both parties consent.

The Processor shall provide its full cooperation in amending and adjusting this DAP in the event of a new privacy legislation.

Following the termination of the **(Insert: Service Level Agreement, Contract etc)** the Processor will delete or return to the Controller all Personal Data in its possession as provided in the DPA except to the extent that the Processor is required by Applicable law to retain some or all the Personal Data (in which case the Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this DPA will continue to apply to such Personal Data.

We hereby agree to the terms of this Data Processing Agreement.

_____	_____
(insert Company Name)	**Kilkenny LEADER Partnership**
_____	_____

(Name of signature Block Caps)

Date: _____

(Name of signature Block Caps)

Date: _____

Appendix A to Data processing agreement

The Data Processor will receive access to the following Personal Data from the Data Controller, in order to deliver its services. Pleas fill in yes or no for each item listed.

Type of Data	**Yes/No**
Name, postal address, phone number, emails	_____
PPS No.	_____
Revenue Information	_____
Bank account details	_____
Pension Details	_____
Proof of Identity (Driving Licence, other id cards)	_____
Leave records	_____
Medical records	_____
Contract of Employment and HR info.	_____
Next of Kin	_____
Family and Dependant info.	_____
Place of employment	_____
Type of employment	_____
Education records	_____
Annual Accounts	_____
Social Welfare information	_____
Client lists	_____
Business Plans	_____
Herd no. Departmental grants etc.	_____
Payments to individuals via grants/ salaries or work undertaken	_____
Other(name)	_____
Other(name)	_____

Appendix 3 Consents for Images etc.

Appendix 3.1 Data Subject Consent From

DATA SUBJECT CONSENT FORM

I, _____ am hereby consenting that _____ can process my personal data/images for the purpose of _____.

I understand that this information has been collected by KLP for their use, and promotion of the company's activities, and will not be passed on to any other organisation for use. All images and data will be stored securely, with restricted access to them, in line with KLP's Data Protection and Photo and Image Polices.

I am aware and I was informed that I may withdraw my consent at any time by using the Data Request Form and contacting the Data Protection Officer, at Kilkenny LEADER Partnership, 8 Patricks Court, Kilkenny in writing or emailing bernie.thorpe@cklp.ie

Signed by: _____

Date:_____

Appendix 3.2 Parental Consent Form

PARENTAL CONSENT FORM

I, _____, confirm that _____ is below the age of 18 years old and I am hereby consenting on his/her behalf that Kilkenny LEADER Partnership can process personal data and the sensitive personal data relating to _____for the purpose of the following as indicated below:

Please tick each appropriate box to indicate that you give consent.

Operational Documents

Contact details, employment records, education records, social welfare records, and any other data which may be required to enable KLP assist them attain their desired outcome. ☐

Please tick each appropriate box to indicate that you give consent.

Photographs/Video

I give permission for my child to be photographed/videoed for use by KLP.
Our team take photographs/videos of the clients these photographs/video are used for recording their learning, reporting to funders, and promoting KLP ☐

I give permission for my child to be photographed/videoed for use outside at events, information sessions and in end of year reports, promoting KLP and its activities. ☐
.

I give permission for my child to be included in photographs that are used online, including our social media platforms. ☐

Note: All photographs will be deleted/destroyed after your child has left the childcare service.

Consent

I am hereby consenting on his/her behalf that KLP can process the Personal Data relating to _____as indicated above. ☐

I am hereby explicitly consenting on his/her behalf that KLP can process the Sensitive Personal Data relating to _____as indicated above. ☐

I am aware that I may withdraw the consent of _____ at any time by using the Data Request Form and contacting the Data Protection Officer, at Kilkenny LEADER Partnership, 8 Patricks Court, Kilkenny in writing or emailing bernie.thorpe@cklp.ie

Signed by Parent/Representative/Legal Guardian,

Signature: Date:

_____ _____

Appendix 3.3 KLP Register of Data Consent for Images

Register of Data Consent for images

Name of person giving consent	Date consent given	Date consent withdrawn	Written Consent on file	Type of images retained photos/ videos etc.	Where images can be displayed	What images can be used for

Appendix 4 Mobile Phone Device Policy.

APPENDIX 4.1 Service restrictions

CORPORATE POLICY ON ACCESS TO DIRECTORY ENQUIRY NUMBERS, PREMIUM RATE NUMBERS and INTERNET

This policy document sets out KLP policy in relation to access by staff to telephoning/texting Directory Enquiry numbers and Premium Dial numbers from landline and Company mobile phones and policy in relation to Internet access on mobile phones.

1. Directory Enquiry Numbers

Examples: **11811, 11850, 11860, 11818, 11890 etc.**

Policy: **Access by staff to dialling Directory Enquiry numbers from landline and Company mobile phones shall be barred.**

Staff should use either hard copy or online telephone directories where possible to locate the required telephone number.

Where access to Directory Enquiries (DE) has been facilitated, staff who dial the DE Service Provider should note the required number and not ask to be put through (i.e. DE providers charge premium rates for connecting calls, so staff should dial

The following on-line directories are available to staff (including staff with restricted desktop internet access):

1. Eircom http://www.eircom.ie/
2. Golden Pages http://www.goldenpages.ie/
3. Kompass http://kompass.business.ie/

In the unlikely event that a number cannot be located as set out above, the staff member can request the number from the switchboard. This should only be necessary in exceptional circumstances.

For those staff members who are away from the office and who require a phone number, it is suggested that you contact the office in order that a colleague may locate the number online for you.

Note: Access to dialling Directory Enquiry numbers shall continue to be made available to Management Team on both landline and Company mobiles, and switchboard staff.

1. MMS and picture message

Sending of MMS messages (save where specifically requested and approved by SMT member for emergency services, cost recovery or enforcement inspection records).

2. Premium Rate Numbers

Examples: **1550, 1530, 1580 etc.**

Policy: **Access by staff to dialling premium rate numbers from landline and Company mobile phones shall be barred.**

Weather information: It is noted that some staff require access to weather forecast information for work purposes. This information is available on http://www.meteireann.ie/ and other weather information websites.

Weather Dial 1550: It is accepted that there may be occasions where access is required to weather forecast information while out of the office. Accordingly, access to Weather Dial Regional Number 1550 123 850 shall be made available to the following staff:

- Management Team
- Other Authorised Employees

3. Special Circumstances

Note: In the event that a staff member requires access to certain information for work purposes, and where such information is only accessible by dialling a premium rate number, the staff member should make a written request to their Line Manager setting out the reason why access to the number is required. The Line Manager should forward his/her recommendation to the CEO/Assistant CEO, for final approval.

Similarly, in the most unlikely scenario where a specific staff member must have access to Directory Enquiries, a similar approach must be followed, and access will only be granted following the approval of the CEO/Assistant CEO.

4 Internet Access

Policy: **Access by staff to internet from Company mobile phones shall be barred for all devices other than where prior approval has been given by CEO/Assistant CEO for business purposes.** Where any User is deemed to be making excessive use of data, such service may be withdrawn**.** In the event of the Company engaging an MDM contractor, any internet access may be forced through the Company's proxy server and all corresponding restrictions applied.

APPENDIX 4.2 Summary responsibilities

User	• Declare and pay for non-work related expenditure, i.e. expenditure in excess of the monthly fixed tariff. • Retain copy receipts for personal contributions paid. • Comply with KLP's Mobile Phone Policy. • In the event of any service requirements for the device, to bring the device to the users base as set out in Appendix 4, by arrangement with the service provider.
Financial Coordinator	• Receive monthly statement of accounts • Check that bills/usage is appropriate • Review monthly exceptions report and arrange follow up action • Approval of team member invoice for payment • Ensure work group names and details are kept up to date (See template in Appendix 4) • Highlight any issues with relevant Line Manager • Monitor usage profile • Monitor monthly
Line Manager	• Liase with the Financial Coordinator re- repayment by users if there is an issue with personal expenditure on the mobile device • Inform the Financial Coordinator in advance when a phone is required for a staff member or there is a change of staff members.
Providers Corporate Affairs	• Overall view of organisational spend and usage profile • Report to SMT on a quarterly basis • Review trends and identify opportunities for savings/efficiencies • Oversight and verification of bill amounts.

Appendix 5 Complaints Form

MODEL COMPLAINT FORM

A: Your details

Surname

Forename(s)

Title: Mr/Mrs/Miss/Ms/if other please state:

Address

Your email address

Daytime phone number

Mobile number

Please state by which of the above methods you would like us to contact you

Your requirements
If our usual way of dealing with complaints is difficult for you, please tell us so that we can discuss how we might help you.

The person who experienced the problem should normally fill in this form. If you are filling this in on behalf of someone else, please fill in section B. Please note that before taking forward the complaint we will need to satisfy ourselves that you have the authority to act on behalf of the person concerned.

B: Making a complaint on behalf of someone else: Their details

Their name in full

Their address

What is your relationship to them?

Why are you making a complaint on their behalf?

C: About your complaint (Please continue your answers to the following questions on a separate sheet(s) if necessary)

What do you think we did wrong, or failed to do?

Describe how you personally or the person you are representing suffered or has been affected

What do you think should be done to put things right?

Have you already put your concern to the frontline staff responsible for delivering the service? If so, please give brief details of how and when you did so.

If you have any documents to support your concern/complaint, please attach them with this form.

Signature:

Date:

When you have completed this form, please send it to:

[Name (Complaints Officer)

[Address and other Contact Details]

Appendix 6 Incident log

Kilkenny LEADER Partnership

Data Incident Log

Log Date	Incident Description	Manual/ Automated?	Personal/ Sensitive?	Encrypted?	Volume of Records	Incident Mgr.	DPC Notified?	Notification Date	Additional Reference material