CONTENTS

HEALTH AND SAFETY POLICY

GENERAL STATEMENT

Our policy is to provide and maintain safe and healthy working conditions and equipment for all our staff, volunteers and directors.

To this end, we will, so far as is reasonably practicable:

- Provide a working environment, equipment and systems of work, which are free from hazard and without risk to health.
- Make arrangements for ensuring safety, and minimise the risk to health in connection with the use, handling, storage and transport of articles and substances. Provide comprehensive information about the risks and necessary precautions.
- Provide such information, instruction, training and supervision as is necessary to ensure the health and safety at work of staff, volunteers and others.
- Ensure that the premises/office(s) under the organisation's control are maintained to an acceptable standard of safety, without risk to health and with adequate access in and out of the premises. Where an office is located within premises of a host organisation ensure that you obtain, read, understand and follow the procedures required by the host organisation.
- Make adequate arrangements for facilities and arrangements for the welfare of employees at work and, if appropriate, health surveillance.
- Provide and maintain arrangements for the emergency evacuation of premises in case of fire or other emergency. Where an office is within premises of a host organisation ensure that you obtain, read and understand these arrangements.

RESPONSIBILITIES

Overall and final responsibility for health and safety in Dalbeattie Community Initiative is that of the Directors of Dalbeattie Community Initiative.

The day-to-day responsibility for health and safety is the volunteer/staff on duty.

All staff and volunteers engaged in the activities of Dalbeattie Community Initiative must be aware of their responsibility:

- To take reasonable care of their own health and safety and for the health and safety of others who may be affected by their acts and/or omissions.
- To co-operate with Dalbeattie Community Initiative in carrying out any duty or requirement imposed on them by statutory measures or by good practice.
- Not to interfere intentionally or recklessly with, or misuse anything provided, in the interest of health, safety or welfare.
- To notify a member of management straight away if they notice a health and safety problem.

CODE OF BEHAVIOUR

VOLUNTEERS AND STAFF

- Complete a registration form and provide references, where appropriate, and work within the aims and objectives of the organisation.
- Use support, guidance and feedback offered and to participate in appropriate induction.
- Keep to agreed commitments and, when unable to do so, inform The Initiative.
- Maintain confidentiality of all privileged information to which they are exposed while serving as volunteer/member of staff.
- Disclose information, which may have an effect on their suitability to volunteer, at any time during their involvement with Dalbeattie Community Initiative. Such information will be dealt with confidentially.

DIRECTORS

- All charity trustees have legal duties and responsibilities. The Directors of Dalbeattie Community Initiative (DCI) are charitable trustees and have duties under company law as well as charity law.

- Purpose of this code: To set out the relevant standards expected by trustees in order to maintain the highest standards of integrity and stewardship; to ensure that DCI is effective, open and accountable; and to ensure a good working relationship between Directors and members of staff

    - Directors must act with probity, due prudence and should take and consider professional advice on anything in which the trustees do not have expertise themselves.
    - A Director must administer the organisation and all its assets in the interest of current, potential and future beneficiaries.
    - Directors should hold themselves accountable to the organisation's stakeholders including the public for the Board's decisions, the performance of the Board and the performance of the organisation.
    - Except where legally authorised, Directors must not gain financial or other material benefit for themselves, their families or their friends from their trusteeship of the charity. Nor must a Director attempt to use his/her status as trustee to gain customer advantage within the organisation i.e. queue jump. The Board should ensure that there are clear written policies on claiming of expenses by Directors.
    - A Director must not place him/herself under any financial or other obligation to outside organisations that might influence him/her in the performance of his/her official duties.
    - Directors should conduct themselves in a manner which does not damage or undermine the reputation of the organisation, or its staff individually or collectively and should not take part in any activity which is in conflict with the objects or which might damage the reputation of the organisation.
    - Directors must make decisions together and take joint responsibility for them. The extent to which any one trustee or small group of trustees is empowered to speak for or take action on

behalf of the organisation or the Board must (subject to any specific constitutional rules) be a matter for all Directors to decide together. Such decisions must be recorded.
    - Directors who sit on the Board as the nominee or representative of a group or organisation must accept that their sole responsibility is to the organisation of which they are trustees, not to their nominated group or body.
- Responsibilities
    - Directors must, with the help of staff, formulate and review regularly the organisation's vision, values, and long-term strategy as well as policies for its fulfilment.
    - With the assistance of staff and appropriate professional advisers, Directors must ensure that the organisation complies with regulatory and statutory requirements and must exercise overall control over the organisation's financial affairs. In addition to compliance with statutory requirements, trustees should have a commitment to the development and implementation of good practice.
    - Directors must be familiar with and keep under regular review the rules and constitution of the organisation. Any changes must be made in accordance with constitutional and legal requirements.
    - In order to develop a working knowledge of the organisation and to give themselves credibility, trustees should endeavour to maintain links and keep in touch with the organisation. Unless there is a good reason to believe that staff actions are threatening the probity of the organisation, all such visits as trustees should be made by arrangement with the appropriate staff member.
- Meetings of the Board of Trustees
    - Directors must strive to attend all meetings regularly, ensuring they prepare for and contribute appropriately and effectively.
    - Directors should bring a fair and open-minded view to all discussions of the Board and should ensure that all decisions are made in the charity's best interests.
    - Directors must aim to foresee and avoid any conflict of interest. Where one arises, a trustee must at once declare the interest and absent him/herself from any discussion or vote taken on the matter by the other trustees. Any transaction under which the trustee will benefit either directly or indirectly must have proper legal authority.
    - Confidential information or material (relating to users, beneficiaries, members, staff, commercial business etc.) provided to or discussed at a Board meeting must remain confidential and within the confines of the Board and must not be discussed outside the Director's body.
    - Directors have a responsibility to develop and ensure the maintenance of a properly constituted, balanced and competent Board, including clear procedures for selection, election, training, retirement and if necessary, removal of trustees and to ensure arrangements are followed for recruiting the Chair, Vice Chair and other honorary officers.
- Staff
    - Directors must ensure there is a clear understanding of the scope of authority delegated to staff members
    - Policies and strategies agreed by Directors should be expressed in unambiguous and practical terms, so that the staff responsible for implementing those policies are clear about what they need to do. Directions given to staff should come from the Board as a whole.
    - Directors should act fairly and in accordance with good employment and equal opportunities principles in making decisions affecting the appointment, recruitment, professional development, appraisal, remuneration and discipline of the staff.

- Directors must understand, accept and respect the difference in roles between the Board, and staff, ensuring that the honorary officers, the Board and staff work effectively and cohesively for the benefit of the organisation, and develop a mutually supportive and loyal relationship.
  Having given the staff delegated authority, Directors should be careful – individually and collectively – not to undermine it by word or action.

FINANCIAL STANDING ORDERS

- These Financial Standing Orders have been accepted by the Board of Directors of Dalbeattie Community Initiative (DCI), and govern the financial practice of DCI, in its task of ensuring its financial management is effective and complies with the relevant legal requirements.
- The Standing Orders may only be amended by DCI Directors by resolution at a formal DCI meeting.
- Aims of the Policy
    - To meet all legal requirements regarding the recording of financial activities.
    - To enable the completion of returns to Companies House and the Charities Regulator
    - To provide information to Funding Bodies
    - To give the Board of Directors control over their finances and enable them to monitor spending and regulate purchases.
    - To ensure that DCI remains financially stable
- Banking
    - Bank Accounts shall only be opened or closed by the Treasurer, with the formal approval of the Board of Directors.
    - Cheque's must be signed by two nominated Directors, and all cheque's will be accompanies by the appropriate certified invoice. Cheque books will be maintained in a secure manner.
    - Changes to the Bank Mandate must be formally approved by the Board of Directors.
    - The Treasurer will be responsible for collecting and banking all monies due to DCI
    - All income must be banked timeously
    - A high interest account will be maintained for funds not immediately required.
- Budgeting
    - The Treasurer, Chair and Business Manager will meet in January of each year, and determine a draft or the Core Cost Budget for the forthcoming year.
    - The Directors of DCI will approve the final draft budget for core costs for the forthcoming year no later than 31st March of each financial year
    - In recognition of the inability of DCI to control the timing of project cost agreement, Directors will approve project budgeting before the commencement of work.
- Expenditure Control
    - The Treasurer will provide statements of Expenditure and Income against budgets each month. He/she will draw Directors attention to significant variations from budget.
    - The Business Manager will maintain a petty cash float not exceeding £100.00. Vouchers which detail expenditure will be presented to the Treasurer when the float requires replenishment.
    - All Expenditure and Income vouchers will be retained for a period of 5 years for annual accounting, audit and income tax purposes.
- Expenses
    - Staff and Volunteers will be able to claim authorised travel and out of pocket expenses, suitably vouched.
    - Rates will be agreed from time to time.
- Insurance
    - The Treasurer will be responsible for ensuring that DCI has adequate insurance for property, third party liability, and employer liability. He/she will notify Directors of new risks, and details will be listed within the Company Annual Report.

- Assets
  - The Company Secretary will maintain a Register of Company Assets, which will be reviewed annually by the Directors.
- Risk Assessment
  - The Business Manager will prepare a policy statement(s) in respect of all activities of DCI, and will identify risk factors which require management arrangements. These will be reviewed annually.
- Reserves Policy
  - The Treasurer will ensure a financial reserves are kept in place, £5700 will be kept as reserves for a 6 month wind down of the company including ensuring the rent payments can be honoured and £22300 will be kept in reserve for salaries notice time and redundancy.

    Reserves breakdown (£):

6 months wages allowance	*19500.00*
Redundancy allowance	*2800.00*
6 month's rent payments	*4800.00*
organisation overheads and accountancy	*900.00*
Total	*28000.00*

EXIT STRATEGY

Dalbeattie Community Initiative is a community based organisation, which is established as a Company limited by guarantee. As such, it has no shareholders, nor is it in financially based partnership with other organisations. It is a registered charity in Scotland and relies on its funding from grants and donations.

- The aim of this strategy is:
  - To consider alternative avenues of funding and the timescales involved.
  - To have an organised procedure for closing the project should the Board of Directors at any time consider the project to be no longer viable.
- Sources of Funding:

  Our expected annual core expenditure is £35,000 with the funding for this budgeted to come from:
  - Generated income (shops) £25,000
  - Other activities including £10,000
    rental income, printing and copying, sponsorship, VIP sales and charges to projects.

  Work is in hand to seek both projects and funding. Potential funding sources are constantly under consideration.
- Closure of the project:
  - In the event that the Directors cannot secure all necessary funding it will consider the individual aspects of the business to establish what cuts in expenditures can be made to allow the self-funding remainder (eg Charity Shop) to continue. Such consideration will be given in consultation with appropriate professional advisers eg Accountants and Solicitors. Care will be taken, as far as possible, to ensure that both financial and non-financial commitments are honoured.
  - In the extreme event that the Directors cannot see sufficient future finance it will need to consider the closure of the company. The Memorandum and Articles of Association are explicit in the broad manner of dissolution of the Company. They state that the winding up of the Company can only take place on the decision of not less than 75% of the ordinary members who are present and voting at a general meeting called for the purpose.
  - Any property remaining after satisfaction of all debts shall be given or transferred to such charitable organisations with similar objects and purposes as may be determined by 75% of the ordinary members present at that meeting.
  - The Company's main financial asset lies in the freehold ownership of its office at 71 High Street, Dalbeattie. The property is not mortgaged. A quick sale would neither be expected nor desired unless the price were acceptable.
  - Every effort will be taken to ensure, as far as is possible, that receipts from the sale of fixed assets, or the transfer of actual property, remain within the ambit and control of the town of Dalbeattie.
  - Assets will be groomed for sale or transfer, to ensure, as far as market conditions allow, that the best values are obtained.
  - Arrangements will be made to give employees adequate notice of closure and to ensure that pay and other benefits as prescribed by Employment Law are honoured.

VOLUNTEERS

THE INTIATIVES COMMITMENT TO VOLUNTEERS

- To recognise the important contribution which volunteers make to the aims and objectives of the organisation.
- Encourages the involvement of volunteers in its work. Staff members are encouraged to assist in the creation of productive volunteer roles that are of benefit to the volunteers and its organisation.

THE INITIATIVE WILL PROVIDE VOLUNTEERS WITH

- Clear role task descriptions and time commitment, outlined either verbally or in written form.
- An induction to the work of The Initiative and preparation appropriate to the nature of the task they will perform.
- A named person who is responsible for providing regular support, guidance and feedback.
- Clear information about out of pocket expenses and simple and straightforward systems for claims and payments.
- A trial period for the benefit of both volunteers and the Initiative to allow both parties to review progress and suitability.
- Opportunities to participate in decision-making where appropriate.
- Information on the insurance cover provided.
- Information and guidance on health and safety.

THE INITIATIVE EXPECTS VOLUNTEERS TO

- Complete a registration form and provide references, where appropriate, and work within the aims and objectives of the organisation.
- Use support, guidance and feedback offered and to participate in appropriate induction.
- Keep to agreed commitments and, when unable to do so, inform the named person of contact.
- Maintain confidentiality of all privileged information to which they are exposed while serving as volunteers.
- Disclose information, which may have an effect on their suitability to volunteer, at any time during their involvement with Dalbeattie Community Initiative. Such information will be dealt with confidentially.

RESOLVING PROBLEMS

- It is hoped that volunteers and Dalbeattie Community Initiative will work co-operatively and that both parties benefit from such work. However, it has to be accepted that problems may occur.
- In order to deal with situations in as positive a way as possible, both parties will be able to use a grievance procedure as detailed in our policies and procedures. The aim of the procedure is to assist both parties to find an acceptable solution to any problems.

RECRUITMENT AND SELECTION OF VOLUNTEERS

- Volunteers will be recruited following the selection procedure and on an equal opportunity basis. The main recruitment measures will be the person's suitability to the task. In the event of a person not suiting the task the Initiative will endeavour to find another suitable task.

RECORDS

- Dalbeattie Community Initiative will set up a record for each volunteer, including dates of services and tasks undertaken, which must be kept up to date and confidential.
- Where appropriate Dalbeattie Community Initiative will provide references for volunteers.
- If required Dalbeattie Community Initiative will set up a record of training and personal development activities undertaken by the volunteer.
- In the event a Personal Development Plan is set up it will be available to said volunteer at any time.

GRIEVANCE PROCEDURE

The Initiative's commitment to provide high quality service and support to our community through our events and projects.

In order to ensure we deliver our highest standards, we have a procedure through which you can let us know of for any reason you are not satisfied with Dalbeattie Community Initiative.

INFORMALLY

- In the first instance you should approach the lead volunteer/staff for the project or event and openly express your grievance verbally.
- The lead volunteer/staff member will try to resolve the issue and come to an agreed solution.
- This interaction will be recorded and reported to Business Manager.

FORMAL COMPLAINT

If you are not satisfied with the informal response and if a solution could not be agreed. The lead volunteer/staff member will advise the grievance should be put in writing.

- A written complaint will raise the matter formally.
- All written complaints should be directed to the Business Manager based at the main office.
- All written complaints will be logged and you will receive written acknowledgement within three working days.
- The complaint will be recorded and reported to Board of Directors.
- The Board of Directors will appoint an investigator to investigate your complaint and give you a written reply within ten working days.
- This reply will set out how the grievance will be dealt with and what action will be taken to resolve the situation.
- In the event that the solution requires further notification to a host/partner organisations all relevant procedures as set out by these organisations will be adhered.

EQUAL OPPORTUNITIES

VOLUNTEERS, STAFF AND DIRECTORS

The operation of DCI is based on the principle of full involvement where everyone, regardless of sex, marital status, disability, special needs, race, colour, religious belief, political belief, sexual orientation, nationality, ethnic origin, age, trade union activity, responsibility for dependants or employment status, has an equal opportunity to contribute and participate in our activities/events/projects.

We are committed to the principle of Equal Opportunities and Diversity and will work towards it in practice as an employer and a community organisation.

AIMS OF THE POLICY

The main aims of the policy are:

1. To promote equality of opportunity and access
2. To eliminate discrimination
3. To provide positive action where appropriate and possible

We will respond and investigate any signs or reports of discrimination and deal with them with appropriate action through our disciplinary procedures.

DCI will ensure all its representatives adhere to the Equal Opportunities policy whilst representing the community.

BARRIERS TO PARTICIPATION

The policy sets out in practical terms the main barriers to participation and seek to identify action for change.

We will ensure that everyone within the DCI organisation has equal access to participation in its representative structures.

It is recognised that the major barriers to participation are:

- Access to information
- Fear of discrimination – stigma and prejudice
- Feelings of exclusion
- Fear of intolerance

We will continually work towards identifying these barriers, eliminating them, and improving our volunteer/staff experiences.

SAFEGUARDING POLICY FOR ADULTS AND CHILDREN

"Dalbeattie Community Initiative believes that children, young people and individuals have a right to be protected from abuse, neglect and exploitation. The welfare of the child, young person and vulnerable adult is the underpinning principle which guides this policy. All staff and volunteers at Dalbeattie Community Initiative have a responsibility to ensure that children, young people and adults receive the best possible service"

SAFEGUARDING IS EVERYONE'S RESPONSIBILITY

Safeguarding of vulnerable adults and ensuring child protection is part of the wider role of safeguarding and promoting welfare. This refers to the activity which is undertaken to protect specific vulnerable adults and children who are suffering or are at risk of suffering significant harm. As adults and/or professionals or volunteers, everyone has a responsibility to safeguard those who are vulnerable and promote their welfare.

Safeguarding and promoting the welfare of vulnerable adults and children – and in particular protecting them from significant harm – depends upon effective joint working between agencies and professionals that have different roles and expertise. Some of the most vulnerable adults, individual children and those at greatest risk of social exclusion, will need co-ordinated help from health, education, children's social care, and quite possibly the voluntary sector and other agencies, including youth justice services.

For those who are suffering, or at risk of suffering significant harm, joint working is essential, to safeguard and promote their welfare and – where necessary – to help bring to justice the perpetrators of crimes against them. All involved should:

- be alert to potential indicators of abuse or neglect;
- be alert to the risks which individual abusers, or potential abusers, may pose to those who are vulnerable;
- share and help to analyse information so that an assessment can be made of the individual's needs and circumstances;
- contribute to whatever actions are needed to safeguard and promote each individual's welfare;
- take part in regularly reviewing the outcomes against specific plans; and
- work co-operatively with parents and/or other carers unless this is inconsistent with ensuring the child's safety.

The Initiative takes seriously the welfare of all vulnerable adults and children who come onto our premises or who are involved in our activities. We aim to ensure that everyone is welcomed into a safe, caring environment with a happy and friendly atmosphere.

INITIATIVE RESPONSIBILITIES

- The Initiative recognises that it the responsibility of each of its staff members, paid or unpaid, to prevent the neglect, physical, sexual or emotional abuse of vulnerable adults or children and to report any abuse discovered or suspected.

- It is the responsibility of the Initiative to implement, maintain and regularly review procedures, which are designed to prevent and to be alert to such abuse.
- The Initiative is committed to supporting, resourcing and training those who work with vulnerable adults or children and to ensure they provide adequate supervision at all times.
- To ensure appropriate checks of staff and volunteers are undertaken if required. In the case of regulated work membership of PVG scheme will be required.

DEFINITIONS OF ABUSE AND NEGLECT:

Abuse and neglect are forms of maltreatment of individuals or children. Somebody may abuse or neglect by inflicting harm, or by failing to act to prevent harm.

Physical abuse

Physical abuse may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating, or otherwise causing physical harm. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces illness in a child.

Emotional Abuse

Emotional abuse is the persistent emotional maltreatment, and for a child to cause severe and persistent adverse effects on the child's emotional development. It may involve conveying that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond the person/child's developmental capability, as well as overprotection and limitation of exploration and learning, or preventing participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying causing person/child to frequently feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment, though it may occur alone.

Sexual Abuse

Sexual abuse of children involves forcing or enticing to take part in sexual activities, including prostitution, whether or not the child is aware of what is happening. The activities may involve physical contact, including penetrative (*e.g.:* rape, buggery or oral sex) or non-penetrative acts. They may include non-contact activities, such as involving children in looking at, or in the production of, pornographic material or watching sexual activities, or encouraging children to behave in sexually inappropriate ways. For vulnerable adults sexual abuse involves forcing or enticing person to take part in sexual activities without consensual agreement.

Neglect

Neglect is the persistent failure to meet basic physical and/or psychological needs; for children this is likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to provide adequate food and clothing, shelter including exclusion from home or abandonment, failing to protect a child from physical and emotional harm or danger, failure to ensure adequate supervision including the use of inadequate care-takers, or the failure to ensure access to appropriate medical care or treatment. It may also include neglect of, or unresponsiveness to emotional needs.

STAFF AWARENESS

All staff will be made aware of this policy as part of their initial induction process and there will be regular briefings and updates for all staff. Where necessary staff or volunteers will be provided with training courses to ensure safeguarding is provided to the highest standard.

PROCEDURES - What to do if you have concerns about an individual or child.

You may have concerns because of something you have seen or heard, or someone may choose to disclose something to you.

If someone discloses information to you:

- Do not promise confidentiality, you have a duty to share this information and refer to social care services.
- Listen to what is being said, without displaying shock or disbelief.
- Accept what is said.
- Give reassurance i.e. "*You're not to blame"*, but only as far as is honest, don't make promises you may not be able to keep e.g. "*Everything will be ok now"* or "*you'll never have to see that person again."*
- Do not interrogate, it is not your responsibility to investigate.
- Do not ask leading questions, ask open questions such as "*anything else to tell me?"*
- Do not ask the individual or child to repeat the disclosure to another member of staff. Telling once is enough.
- Explain what you have to do next and who you have to share the information with.
- Take notes if possible or write up your conversation as soon as possible afterwards.
- Record the date, time, place any non-verbal behaviour and the words used by the individual (do not paraphrase)
- Record statements and observable things rather than interpretations or assumptions.

Whatever the nature of the concern, discuss them with the designated safeguarding member of staff immediately.

The safeguarding officer will then:

- Complete an incident report with required actions.
- These will then be agreed by safeguarding officer and chairman.
- If required relevant agencies will be contacted (Police, Social services etc.).
- In the event that the solution requires further notification to a host/partner organisations all relevant procedures as set out by these organisations will be adhered.

Process diagram:

There are concerns/suspicions about a person's behaviour, or

There has been a disclosure or an allegation about a person's behaviour.

- Acknowledge information about allegations or concerns of abuse.
- Take the person seriously and refer to the notes within this policy.

- Ensure the immediate safety of the child or vulnerable adult.
- In an emergency when someone is at risk, contact Police and/or medical services.

- As soon as possible, make a record of what has been said, heard, and/or seen.
- Sign and date the record.
- Do not investigate the situation.

- Pass all the information to the designated safeguarding officer.
- The safeguarding officer (or in the event the safeguarding officer is implicated, the Chairman) will investigate.
- An incident report will be completed and actions agreed by safeguarding officer and chairman.
- If required relevant agencies will be contacted.
- In the event that the solution requires further notification to a host/partner organisations all relevant procedures as set out by these organisations will be adhered.

Possible outcomes:

Criminal proceedings, Police enquiry, Disciplinary Measures, putting together a case management group to decide on the management of any remaining concerns, or no further action required. (This is not an exhaustive list)

EMPLOYED STAFF

INTRODUCTION

- Dalbeattie Community Initiative (DCI) is committed to supporting and developing its staff/volunteers to enable them to carry out their work effectively and to fulfil their potential.
- It is the aim of this policy to ensure that staff expect and receive appropriate support and training to enable them to do their job, meet agreed objectives, improve performance, and develop skills and knowledge.
- Line managers are responsible for providing both support and development opportunities. This is done both informally, in the course of everyday communication, and more formally through induction, day to day line management, and regular support and supervision.

PURPOSE OF APPRAISAL

- Appraisal allows the opportunity to Look Back and to Look Forward - very much in line with the words in the Dalbeattie Town crest.
- The purpose of the appraisal meeting is to;
  - clarify objectives,
  - identify changes in the nature of the work done and possible new directions,
  - help staff to make the most of themselves by reviewing their strengths and weaknesses with a view to planning action to assist development,
  - increase the effectiveness of the organisation. This might include changes in work practice, identification of training needs, and consideration of long-term plans,
  - inform future supervision sessions – for example, to measure and build upon progress on agreed items
  - consider training needs where appropriate.

THE APPRAISAL PROCEDURE

- The basis of the system is that each employee has a major role to play in their own appraisal.
- Accordingly, all appraisals will be conducted in such a way that an honest exchange of views is encouraged. The whole process will feel genuinely two-way, and both participation and openness is a requirement.
- The meeting will take place in comfortable surroundings, and timed to remain free from interruptions.
- Is an annual meeting between the employee and his/her line Manager and both the employee and their manager will complete a pre-appraisal form. These forms are for the benefit of both the person carrying out the appraisal and the person being appraised to outline the areas they wish to cover.
- The employee and the manager each give the other party a copy of their pre-appraisal form at least three (3) days prior to the appraisal meeting so that the points they contain can be considered. This exchange of forms must take place at the same time.
- The appraisal process is a positive way of helping people to develop their potential whilst carrying out their work. Benefits to the person being appraised include the chance to:
  - discuss how he/she is getting on with the work in detail
  - find out the line manager's views of his/her work
  - explore ways of working more effectively
  - discuss his/her future within the organisation
  - discuss how he/she sees his/her career developing
  - share views on how he/she sees he/she is being managed
  - Give feedback to his/her manager.

- The two parties should agree actions to be taken as a result of the meeting and agreements on action points should be recorded in writing, using the Appraisal Form so that, if necessary, these can be referred to in subsequent meetings
- All staff are to be appraised under this system, including the Chief Executive, who should be appraised by the Chair and/or other designated Board member.

APPRAISAL TIMESCALES

- The first appraisal takes place 6-9 months after a new employee has started;
- Thereafter appraisals should be completed annually during September of each year

CONFIDENTIALITY

- The Appraisal Form is seen by the relevant member of staff, the line manager and the Chair. The Appraisal Form will be retained on file for reference on future appraisals, including by a future line manager.

DISAGREEMENTS

- Both parties should agree that the Appraisal Form accurately reflects the discussions and, where appropriate, describes any disagreements. Frequently, disagreements simply reflect areas which need to be taken forward to a future meeting.
- However, if necessary, any appraisee who feels that his/her appraisal was unsatisfactory or unfair to him/her, may ask that a senior manager /Director to review the appraisal with him/her and the appraiser.
- Ultimately, the employee has the right to raise a grievance in relation to any aspect of the appraisal system.

DISCIPLINARY PROCEDURE

INTRODUCTION

- The purpose of the Disciplinary Procedure is to help and encourage all employees to achieve and maintain required standards of conduct, job performance and good discipline. It is also a statutory requirement when contemplating disciplinary action including dismissal of an employee.
- It seeks to enable the individual whose performance and/or conduct has failed to reach the required standard, to make the necessary improvement through guided instruction. The aim is to ensure that the organisation's interests are safeguarded while staff are treated fairly and equitably, with an emphasis on correction rather than punishment.

PRINCIPLES

This procedure will work in accordance with the following principles:

Informal action

- Since it is the aim of DCI to encourage acceptable standards of conduct and performance, every effort will be made to deal with relatively minor problems informally by the supervisor/line manager with the aim of avoiding the need to implement the formal procedure. This will include setting clearly defined objectives and standards, and monitoring them over a reasonable time period. The supervisor will arrange for provision of support, practical assistance and/or training as appropriate to ensure that acceptable standards of work performance and behavior are met.

Investigation

- This procedure is designed to establish the facts of any matter quickly, and to deal consistently with disciplinary issues. No formal disciplinary action will be taken until a full investigation has been carried out. Written records of all investigations will be kept including notes of any investigatory meetings held to establish the facts of the case. At the investigatory stage it will be made clear to the employee that it is not a disciplinary hearing and that the decision at the end of the investigation will be to:
  (1) Drop the matter
  (2) Use the informal process
  (3) Use the formal disciplinary process

The right to be accompanied

- At all stages of the formal disciplinary procedure employees have the right to be accompanied by a work colleague, friend, or trade union representative. Before any meetings take place the employee should tell the employer whom they have chosen as a companion. The companion will be allowed to address the hearing in order to:
  (1) Put the employee's case
  (2) Summarise the employee's case
  (3) Respond on the employee's behalf to any views expressed at the hearing
  (4) Confer with the employee
  (5) Ask witnesses questions if required
- It will not be acceptable for the companion to:
  (1) Answer questions on the employee's behalf
  (2) Address the hearing against the wishes of the employee
  (3) Prevent the organisation from explaining their case

- Should the companion attempt to act out with their remit or display signs of aggressive and/or disruptive behaviour the meeting will be adjourned until the companion agrees to comply with their remit or a replacement companion be found.

Right to appeal

- At all stages of the formal disciplinary procedure employees have the right to appeal against any disciplinary action taken.

Disability

- At all times during any informal or formal proceedings the organisation will ensure, where they know an employee has a disability, to make any possible reasonable adjustments to ensure the procedure is fully accessible and understandable to all employees. These adjustments may include but are not limited to:
  (1) Location and timing of meetings
  (2) Alternative formats of all written disciplinary information
  (3) Equipment such as an induction loop, sign language interpreter
  (4) Appropriate adjustments for people with a learning disability

Records

- Accurate records will be kept at each stage of the procedure. These will be stored confidentially and retained in accordance with the timescales noted in this procedure and the Data Protection Act 1998.

Implementation stage

- The procedure may be implemented at Stage 1, 2 or 3 if the alleged misconduct warrants such action. For example, where there is evidence of gross misconduct the employee may be dismissed.

Timescales

- All timescales mentioned in relation to arranging hearings and giving decisions are subject to change in the event that particular circumstances prevent them being adhered to.

FORMAL PROCEDURE

Where an informal approach fails, or the matter is more serious, the following formal procedure will be used.

- Investigation
  - The person/s designated to investigate will identify and clarify the issue by establishing the essence of the problem. The matter must be investigated in a systematic and thorough manner by gathering information promptly, establishing relevant facts and taking into account statements of witnesses if appropriate.
  - The employee will be expected to attend any investigatory meeting called.
- Suspension
  - In serious cases, the Management Committee will have the power to suspend the employee, with full pay, pending investigation of the allegations. Suspension in these circumstances does not constitute disciplinary action. The employee will be informed in writing of the reasons for the suspension. Any suspension will be to allow a full investigation to be completed and will be conducted as efficiently as possible, the employee will be suspended for as short a period as possible to allow the investigation to be completed.
- Disciplinary Hearing
  - Following the investigation if a disciplinary hearing is warranted, the employee should, within 5 working days, be given a written statement of the allegation and advised of the intention to hold

a disciplinary hearing. The statement will detail the date, time and location of the disciplinary hearing and who will be present. The statement will set out the employee's rights under this procedure, including the right to be accompanied by a trade union representative or work colleague and the right to an appeal. The employee will be provided with copies of all documentation and supporting evidence to be presented by the employer at the hearing, including details of any witnesses or witness statements prior to the hearing, as appropriate.

- If the employee's chosen companion is unavailable to attend on the date or at the time originally set for the hearing, the employer must postpone the meeting to another date and time proposed by the employee within five working days of the date proposed by the employer.
- On conclusion of the disciplinary hearing the employee will be advised in writing, within 5 working days, of the outcome of the hearing and any disciplinary sanctions to be applied.

DISCIPLINARY SANCTIONS

Depending on the circumstances, one of the following range of disciplinary sanctions may be applied:

- Stage 1 - First Written Warning

  If conduct or performance is unsatisfactory, a first written warning will be issued. This will be confirmed in writing, and recorded. The written warning will give details of the complaint, the improvement or change in behaviour required, the timescale, if any, allowed for this, the employee's right of appeal, and whether a final written warning may be considered if there is no sustained improvement or change. The warning will be disregarded after 6 months if satisfactory service is achieved and maintained.

- Stage 2 – Final Written Warning

  If an offence is sufficiently serious, or no improvement has been made, or a further offence occurs, a final written warning will be issued. This should detail the nature of the misconduct in question (or evidence of a continuing deterioration in performance); specify the time limits within which improvements are to be effected; and remind the employee of his or her right to appeal. This will remain on record for 12 months, and will make it clear that a failure to improve, repetition of the offence, or other misconduct will result in dismissal.

- Stage 3 – Dismissal

  If there is no satisfactory improvement, or if further misconduct occurs, the employee will be dismissed. The letter should specify the reasons for the dismissal, the date on which the dismissal is to take effect, and the appropriate period of notice (or pay in lieu of notice). It should also remind the employee of his or her right of appeal.

GROSS MISCONDUCT

If, after investigation, and a disciplinary hearing, it is confirmed that the employee has committed gross misconduct, the normal outcome will be dismissal without notice.
Examples of gross misconduct are listed below under Disciplinary Offences.

APPEALS

- If an employee wishes to appeal against any disciplinary decision, which has been taken, they must do so in writing to the Chairman within 10 working days of being notified of that decision. The employee should make clear the reasons for their appeal. If possible, a person or persons who have had no direct involvement in the disciplinary action being appealed will hear the appeal.
- The appeal hearing will be arranged as soon as possible, and in any event no longer than 10 working days from the receipt of notice of appeal. The employee will be informed of the outcome of the appeal within 5 working days of the hearing.
- The outcome of the appeal hearing will be final.
- Employees should note that an appeal hearing is not intended to repeat the detailed investigation of the disciplinary hearing, but to focus on specific factors which the employee feels have been dealt with unfairly or which have received insufficient consideration, such as:
  - an inconsistent, inappropriate or excessively harsh penalty
  - extenuating circumstances
  - bias of the disciplining manager
  - unfairness in the conduct of the hearing
  - new evidence subsequently coming to light.
- Where new evidence arises during the appeal, the employee should be given the opportunity to comment on this before any action is taken. It may be appropriate to adjourn the appeal to consider any new evidence that arises.
- Where an appeal against dismissal fails, the effective date of termination will be the date on which the employee was originally dismissed.

DISCIPLINARY OFFENCES

- Misconduct is defined as failure in personal conduct, persistent poor performance or deliberate infringement of policies, rules and procedures. The decision to take disciplinary action or the sanction imposed may vary according to the exact circumstances of the case. Reasons for disciplinary action may include but are not limited to:
  - Dishonesty
  - Breach of confidentiality
  - Misuse, unauthorised use of, or reckless damage to the organisation's property, including equipment, materials and information
  - Health and safety issues, for example
  - Threatened physical assault;
  - Abusive behaviour, offensive or obscene language or gestures directed at employees; members of the Management Committee; members of the public;
  - Failure to observe established health, fire and safety rules and to report accidents or injuries whilst on duty;
  - Smoking in any other than designated areas;
  - Oppressive or abusive conduct; bullying, harassment or victimisation;
  - Performance related issues, for example:
  - Neglect of duty which undermines the organisation;
  - Failure over a period of time to perform work to satisfactory standards;
  - Failure to carry out duties effectively while under the influence of alcohol or drugs, other than medically prescribed;
  - Refusal to carry out a reasonable order of a manager;

- Infringement of terms and conditions of service, for example :
  - Persistent lateness;
  - Unauthorised absence;
  - Excessive sickness absences with no appropriate certificates or authorisation;
  - Failure to comply with policies, procedures and regulations as laid down by the employer from time to time;
  - Engaging in or knowledge of activities on or off the premises which could be considered a discredit to the organisation or its employees;
  - Undertaking additional employment which would counter the interests of the organisation or would conflict with the employee's own position;
  - Making unauthorised statements to the press or news media relating to the organisation's business.

GROSS MISCONDUCT

- Gross misconduct is defined as misconduct serious enough to destroy the employment contract between the organisation and the employee, which makes further working relationship and trust impossible. Gross misconduct is normally restricted to serious offences. The principal reasons for summary dismissal could include but are not limited to:
  - Criminal offence which affects the individual's ability to carry out his/her job;
  - Physical assault by an employee on any other person
  - Theft, misappropriation or unlawful destruction of property: the employer's, employees' or others'
  - Serious infringement of safety rules or negligence which causes unacceptable loss, damage or injury
  - Supplying security access codes to any unauthorised person
  - Unauthorised disclosure of information or misuse of trust of a serious nature
  - Making malicious or unfounded allegations of a serious nature
  - Deliberate falsification of any documents or claims, including time sheets, overtime or expense forms
  - Misconduct at work or away from work of such a serious nature as to bring into disrepute either the employee's position or the organisation
  - Unlawful discrimination, harassment, victimisation or bullying
  - Alcohol or drug abuse
  - Failure to disclose unspent criminal conviction(s) or any convictions, whether spent or not, in respect of posts exempt under the terms of the Rehabilitation of Offenders Act 1975;
  - Providing false information on a job application form.

MANAGING INFORMATION AND DATA

Three documents have been produced in order to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR').

- Data Protection Policy
- Data Privacy Notice
- Data Protection Guidelines for Employees, Volunteers and Consultants.

DATA PROTECTION POLICY

1. **Introduction**

This Policy sets out the obligations of Dalbeattie Community Initiative Ltd (the Company) regarding data protection and the rights of its data subjects in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

The GDPR defines personal data as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. **The Data Protection Principles**

2.1 This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.1.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.1.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.1.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

3.1 The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1.1 The right to be informed;

3.1.2 The right of access;

3.1.3 The right to rectification;

3.1.4 The right to erasure (also known as the 'right to be forgotten');

3.1.5 The right to restrict processing;

3.1.6 The right to data portability;

3.1.7 The right to object;

3.1.8 Rights with respect to automated decision-making and profiling.

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject;

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in the Company's Privacy Notice. This includes:

5.1.1 Personal data collected directly from data subjects**;**

5.1.2 Personal data obtained from third parties.

5.2 The Company only collects, processes, and holds personal data for the specific purposes as set out in the Company's Privacy Notice (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

6. Adequate, Relevant, and Limited Data Processing

6.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Process included within our Privacy Notice.

9. Secure Processing

9.1. The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided.

10. Accountability and Record-Keeping

10.1 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.1.1 The name and details of the Company, and any applicable third-party data processors;

10.1.2 The purposes for which the Company collects, holds, and processes personal data;

10.1.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

10.1.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.1.5 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Process located within the Privacy Notice);

10.1.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR**.**

11.2 Data Protection Impact Assessments shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided via access to the Privacy Notice which provides all of the information below this will be a link on our website or hard copy at request:

12.2.1 Details of the Company;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the EEA), details of that transfer, including but not limited to the safeguards in place;

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the supervisory authority under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests (SARs) at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Data subjects wishing to make a SAR may do so in writing, using the Company's Subject Access Request Form, or other written communication. SARs should be addressed to the Company Secretary.

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation**.**

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Objections to Personal Data Processing

17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

17.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18. Data Security - Transferring Personal Data and Communications

18.1 The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

18.1.1 All emails containing personal data must be marked "confidential" and deleted once the personal data is stored securely;

18.1.2 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

18.1.3 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

19. Data Security - Storage

19.1 The Company shall ensure that the following measures are taken with respect to the storage of personal data:

19.1.1 All electronic copies of personal data should be stored securely using passwords and data encryption where applicable;

19.1.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely or locked away;

19.1.3 All personal data stored electronically should be backed up regularly. All backups should be encrypted where necessary;

19.1.4 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

20. **Data Security - Disposal**

20.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Process included within the Privacy Notice.

21. **Data Security - Use of Personal Data**

21.1 The Company shall ensure that the following measures are taken with respect to the use of personal data1

21.1.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Company Secretary;

21.1.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Company Secretary;

21.1.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

21.1.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

21.1.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Company Secretary to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

22 **Implementation of Policy**

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

DATA PRIVACY NOTICE

1 Introduction

This Policy sets out the obligations of Dalbeattie Community Initiative Ltd (the Company) regarding data protection and the rights of its data subjects in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

The GDPR defines personal data as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

2.2 This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

3.2 The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.2.1 The right to be informed;

3.2.2 The right of access;

3.2.3 The right to rectification;

3.2.4 The right to erasure (also known as the 'right to be forgotten');

3.2.5 The right to restrict processing;

3.2.6 The right to data portability;

3.2.7 The right to object;

3.2.8 Rights with respect to automated decision-making and profiling.

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject;

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in the Company's Privacy Notice. This includes:

5.1.1 Personal data collected directly from data subjects**;**

5.1.2 Personal data obtained from third parties.

5.2 The Company only collects, processes, and holds personal data for the specific purposes as set out in the Company's Privacy Notice (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

6. Adequate, Relevant, and Limited Data Processing

6.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Process included within our Privacy Notice.

9. Secure Processing

9.1. The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided.

10. Accountability and Record-Keeping

10.1 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.1.1 The name and details of the Company, and any applicable third-party data processors;

10.1.2 The purposes for which the Company collects, holds, and processes personal data;

10.1.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

10.1.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.1.5 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Process located within the Privacy Notice);

10.1.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR**.**

11.2 Data Protection Impact Assessments shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided via access to the Privacy Notice which provides all of the information below this will be a link on our website or hard copy at request:

12.2.1 Details of the Company;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the EEA), details of that transfer, including but not limited to the safeguards in place;

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the supervisory authority under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests (SARs) at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Data subjects wishing to make a SAR may do so in writing, using the Company's Subject Access Request Form, or other written communication. SARs should be addressed to the Company Secretary.

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Objections to Personal Data Processing

17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

17.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18. Data Security - Transferring Personal Data and Communications

18.2 The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

18.2.1 All emails containing personal data must be marked "confidential" and deleted once the personal data is stored securely;

18.2.2 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

18.2.3 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

19. Data Security - Storage

19.2 The Company shall ensure that the following measures are taken with respect to the storage of personal data:

19.2.1 All electronic copies of personal data should be stored securely using passwords and data encryption where applicable;

19.2.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely or locked away;

19.2.3 All personal data stored electronically should be backed up regularly. All backups should be encrypted where necessary;

19.2.4 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

20. Data Security - Disposal

20.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Process included within the Privacy Notice.

21. Data Security - Use of Personal Data

21.1 The Company shall ensure that the following measures are taken with respect to the use of personal data1

21.1.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Company Secretary;

21.1.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Company Secretary;

i. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

ii. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

iii. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility

of the Company Secretary to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

22 **Implementation of Policy**

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

DATA PROTECTION GUIDELINES FOR EMPLOYEES, VOLUNTEERS AND CONSULTANTS

1 Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside any other notice we issue to you in the future in relation to your data.

1.3 The Company has measures in place to protect the security of your data in accordance with our current Data Protection policy. A copy of this can be obtained from the Business Manager.

1.4 The company will hold data in accordance with our Data Retention Policy which is included in our Privacy Notice. A copy of this can be obtained from our page on Dalbeattie Matters. We will only hold data for as long as necessary for the purposes for which we collected it.

1.5 The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.6 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

1.7 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;

- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us (if required);
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your trade union membership;
- your health;
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 How will we process your personal data?

5.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

5.2 We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

6 When we might process your personal data

6.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

6.2 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Company Secretary.

6.3 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

6.4 We do not take automated decisions about you using your personal data or use profiling in relation to you.

7 Sharing your personal data

7.1 Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

7.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

7.3 Farries Kirk and McVean will hold employee details in the accordance to GDPR regulations and inline with our own policy in relation to payroll.

7.4 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

8 **How should you process personal data for the Company?**

8.1 Everyone who works for, or on behalf of, Dalbeattie Community Initiative (employee, volunteer and contractor) has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Protection, Privacy Notice and Data Retention policies.

8.2 The Company's Data Protection Officer (The Company Secretary) and Business Manager (Michelle McRobert) are responsible for reviewing this policy and updating the Board of Directors/Trustees on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to these persons.

8.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

8.4 You should not share personal data informally.

8.5 You should keep personal data secure and not share it with unauthorised people.

8.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

8.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

8.8 You should use strong passwords.

8.9 You should lock your computer screens when not at your desk.

8.10 Personal data should be encrypted before being transferred electronically to authorised external contacts.

8.11 Do not save personal data to your own personal computers or other devices.

8.12 Personal data should never be transferred outside the European Economic Area.

8.13 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

8.14 You should not take personal data away from Company's premises without authorisation from the Business Manager/The Company Secretary.

8.15 Personal data should be shredded and disposed of securely when you have finished with it.

8.16 You should ask for help from our Data Protection Officer/Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

8.17 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

8.18 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

9 How to deal with data breaches

9.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

9.2 If you are aware of a data breach you must contact the Company Secretary immediately and keep any evidence you have in relation to the breach.

10 Subject access requests

10.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Company Secretary who will coordinate a response.

10.2 If you would like to make a SAR in relation to your own personal data you should make this in writing as above. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

10.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

11 Your data subject rights

11.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

11.2 You have the right to access your own personal data by way of a subject access request (see above).

11.3 You can correct any inaccuracies in your personal data. To do you should contact the Company Secretary.

11.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact The Company Secretary.

11.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Company Secretary.

11.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

11.7 You have the right to object if we process your personal data for the purposes of direct marketing.

11.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

11.9 With some exceptions, you have the right not to be subjected to automated decision-making.

11.10 You have the right to be notified of a data security breach concerning your personal data.

11.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Company Secretary.

11.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly.

SOCIAL MEDIA POLICY

This social media policy describes the rules governing the use of social media at Dalbeattie Community Initiative.

Social media can bring significant benefits to our organisation, particularly for creating online conversations with our community members. However it is important that staff/volunteers who use social media do so in a way that enhances the DCI and the community's prospects. A misjudged status update can generate complaints or damage our reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively. It applies whether the social media use takes place in the work place or whilst working from home.

RESPONSIBILITIES

Everyone who has authority as admin, editor or page host on a project/event social media account connected to Dalbeattie Community Initiative has responsibility for implementing this policy.

- The Business Manager is ultimately responsible for ensuring that Dalbeattie Community Initiative uses social media safely, appropriately and in line with the organisation's objectives.
- The Business Manager is also responsible for proactively monitoring for social media security threats.
- It is everyone's responsibility to ensure requests for information, assistance, and support via social media are followed up.

In the event of any issues arising from a social media account or breaches in the policy the directors will have the final decision on what action is required – this may include the closure of the social media accounts.

GUIDELINES

- There will be a minimum of two persons as administrators on each page/account to ensure the organisation have access to the accounts at all times. The Business Manager will keep details of all accounts, access and appointed administrators.
- Creation of new social media accounts should not be made unless approved by the directors at a monthly meeting – and the agreement noted in the minutes.
- Understand the social network: spend some time becoming familiar with the social network before contributing. It's important to read any FAQ's and understand what is and is not acceptable on the platform before posting messages or updates.
- Keep within policy: No posts, status updates or shared links should contain any inappropriate content. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Be polite: Never interact in a way that could be interpreted as being offensive, disrespectful or rude.
- If unsure, don't post it: Staff/volunteers should err on the side of caution when posting. If you think an update or a message might cause complaints or offense – or be otherwise unsuitable – please do not post it and consult a member of the management team for advice.
- Don't escalate: Take time to think before responding. If in doubt hold back, be thoughtful and polite. If there is a complex issue or complaint always make further communication via email or in person in order to resolve the situation and include the Business Manager or a director in the conversation.

BREACHING THE POLICY

Knowingly breaching this social media policy will be taken seriously. Any staff/volunteers who do so will be subject to disciplinary action. If appropriate we will involve the police and/or other law enforcement agencies in relation to breaches of this policy.

END