## Contents

## Introduction

Windmill Hill City Farm is registered with the Information Commissioners Office (https://ico.org.uk/) under registration number Z9491512. This registration is renewed annually in May.

For the purposes of administration and the management of the business Windmill Hill City Farm needs to retain and process personal information about its employees, volunteers, clients, suppliers and other contacts. Some areas of the organisation (child care and adult health & social care in particular) have specific information handling requirements over those generally applicable. Windmill Hill City Farm is committed to ensuring that all personal information is processed fairly, lawfully and as transparently as possible and is compliant with the General Data Protection Regulation (GDPR) effective from 25 May 2018.

## Policy

All staff, trustees and volunteers will be made aware of this policy when joining the organisation through the induction process. For the purpose of this policy the word employee will apply to employees and volunteers (including trustees).

This policy draws on advice issued by the Information Commissioner at https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf.

Article 5 of the GDPR requires that personal data shall be

> (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> (b) 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;
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 individuals;

(f) 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.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The GDPR provides the following rights for individuals:

1. The right of access
2. The right to rectification
3. The right to erasure
4. The right to restrict processing
5. The right to data portability
6. The right to object
7. Rights in relation to automated decision making and profiling.
8. The right to be informed

As a data controller, Windmill Hill City Farm must appoint a Data Protection Officer if it meets the following criteria

- is a public authority (except for courts acting in their judicial capacity);
- carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

None of these criteria currently apply. We do not therefore have an appointed Data Protection Officer.

## Customer Data

The data of clients, customers and service users is handled in a manner compliant with the GDPR of 2018. A general privacy statement (see Appendix B) describes the manner in which we handle client data.

## Employee Data

Information is kept about employees for legal purposes (eg for payroll), for administration purposes and for the purposes of day-to-day management. The organisation will process the information in your employment record in accordance with its Employee Privacy Notice which may be revised and re-issued from time-to-time.

## Employee Privacy Notice

This notice provides employees with information about how their personal data will be used during their employment with the organisation.

Data controller: Sarah Mellor, Office Manager

The organisation collects and processes personal data relating its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

Information the organisation collects

The organisation collects and processes a range of information about employees. This includes

- name, address and contact details, including email address and telephone number, date of birth and gender;
- terms and conditions of employment;
- details of qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of bank accounts and national insurance number;
- information about marital status, next of kin, dependants and emergency contacts;
- information about nationality and entitlement to work in the UK;
- information about criminal record;
- details of work schedule (days of work and working hours) and attendance at work;
- details of periods of leave, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures, including any warnings issued and related correspondence;
- assessments of performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- information about medical or health conditions, including disability for which the organisation needs to make reasonable adjustments; and
- equal opportunities monitoring information including information about ethnic origin, sexual orientation and religion or belief.

The organisation may collect this information in a variety of ways. For example, data might be collected through application forms, CV, obtained from passports or other identity documents, from forms completed during employment (such as benefit nomination forms), from correspondence or through interviews, meetings or other assessments.

In some cases, the organisation may collect personal data from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

Data will be stored in a range of different places, including personnel files, HR management systems and in other IT systems (including the email system).

Why the organisation processes personal data

The organisation needs to process data to enter into an employment contract with employees and to meet its obligations under such contracts. In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations, eg, to check an employee's entitlement to work in the UK.

The organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows it to

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current/former employees or for mortgage applications; and
- respond to and defend against legal claims.

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where the Organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out its obligations and exercise specific rights in relation to employment.

Who has access to data

Personal information may be shared internally, including with members of the HR and recruitment team (including payroll), line managers, managers in the business area in which an employee works and IT staff, (if access to the data is necessary for performance of the role).

WHCF shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. WHCF may also share your data with third

parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

WHCF also shares your data with third parties that process data on its behalf:

| **Company – 3rd party** | **Data processed** |
|---|---|
| Godfrey Wilson Accountants | Payroll<br><br>All Accounting matters. |
| Amba | HR Support and Consulting |
| Security Watchdog Part of Capita plc | DBS checking |
| Cyclescheme | Cycle to work scheme – salary sacrifice scheme |
| Complete IT | Has access to data through its role as IT support |

WHCF will not transfer your data to countries outside the European Economic Area.

How the organisation protects data

The organisation takes the security of personal data seriously. It has internal policies and controls in place to try to ensure that data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties

Where the Organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Organisation measures to ensure the security of data.

How long the organisation keeps data

The Organisation will hold personal data for the duration of an employee's employment. The periods for which data is held after the end of employment are given in Appendix A.

Employee rights

As a data subject, employees have a number of rights:

- access and obtain a copy of your data on request;
- require the Organisation to change incorrect or incomplete data;
- require the Organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the Organisation is relying on its legitimate interests as the legal ground for processing.

Employees may exercise these rights by contacting the data controller. If they believe that the organisation has not complied with data protection rights, they can complain to the Information Commissioner.

Employee obligations

In connection with their own personal data all employees have a duty to; check that any information that they provide to the Farm in connection with their employment is accurate and up to date; inform the Farm of any changes or errors in information which they have provided eg change of address (the Farm cannot be held accountable for errors arising from changes about which it has not been informed).

All personal data should be accessible to only those who need to use it. It should be stored in a secure environment, be password protected if computerised and only kept on portable storage media where absolutely necessary. All portable storage media containing personal data must be kept in a secure place.

Employees have obligations under their employment contract to provide the organisation with data. In particular, they are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. They may also have to provide the organisation with data in order to exercise their statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that they are unable to exercise your statutory rights.

Certain information, such as contact details, proof of the right to work in the UK and payment details, must be provided to enable the organisation to enter a contract of employment. Not providing other information, will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

In the course of their employment employees may have access to personal information of other employees, customers and other contacts. Employees must follow the procedures on dealing with personal information to ensure that a breach of the GDPR, this policy and other related legislation does not occur. Personal Data should only be used in accordance with our Data Protection policy. Use of data for anything which is not necessary for the performance of the job will be subject to disciplinary proceedings.

Automated decision-making

Employment decisions are not based on automated decision-making.

Monitoring

The organisation reserves the right to monitor email communications, internet usage and telephone calls to ensure responsible usage or where it feels that the business tools provided are being used for purposes other than business use. As such you should be aware that communications in the work environment may not remain private.

## Client Data

Personal Information is gathered from visitors and activity participants only in so far as is essential for the administration of the services offered. There are two client groups to which specific regulation applies: Children in the Nursery (and associated services) and Health & Social Care clients.

### Children's Data

Administrative data for the families registered in the Children and Family Services is held on the local server and administered through the commercial 'First Steps' software. Learning diaries for the children are

hosted on a web-based application called 'Tapestry' which implements a high standard of security (ISO27001 compliant – see GN11a Tapestry Security Policy). Paper files (eg registration, consent forms) are kept in a looked filing cabinet in the Nursery office.

### Health & Social Care Clients

In the case of Health and Social Care clients additional regulations apply as a 'care organisation'. These are determined by NHS Digital Home - NHS Digital and include those instigated from the 'Caldicott Review' in 1997 and its follow up report in 2012.

The Farm follows the 'Caldicott' Principles in gathering and using client data, namely

- Justify the purpose(s) of using confidential information
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need-to-know basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect confidentiality

The governance of information is guided by the Data Security and Protection Toolkit published by NHS Digital. It requires use of an information governance improvement plan. This is appended to this policy.

## Accessing Data

The Farm upon request will confirm what personal data they hold in relation to an employee or client. Subject to any statutory exemptions all employees and clients shall be entitled to request access any personal data or sensitive personal data the Farm have retained in relation to the requesting individual.

Any employee or client shall also be able to request the Farm amend or correct inaccurate information retained. An employee or client wishing to make such a request must provide details in writing to their line manager or contact point outlining the disclosure sought.

The Farm will process any request without unreasonable delay and in any event within one month of the Farm having receipt of the written request and any additional information which the Farm reasonably requires in order to locate the information. No obligation upon the Farm to provide the information arises until these conditions have been fulfilled.

Where the requesting employee or client has failed to provide sufficient information to readily identify the data sought the Farm may write back requesting further details. The information will be supplied by way of a copy, except where the supply of a copy in permanent form is not possible or would involve disproportionate effort, or the employee agrees otherwise. The Farm shall provide access to the information unless doing so would infringe upon the rights of any third party or any legal exemption applies.

## Sharing information

Sometimes, situations may arise where it would be appropriate to break confidentiality or share information. Circumstances which may be considered as appropriate are as follows:

- Where the information is not personal or confidential in nature;
- Where the person to whom the duty is owed has given explicit consent (eg through the sign-up form for services)
- Where there is an overriding public interest in disclosure;
- Where it is considered that withholding information could cause harm or injury to someone
- Where there is a legal obligation to disclose information for example
  - It is disclosed or considered that a criminal offence has been or will be committed.
  - Information disclosed relating to acts of terrorism
  - Disclosure of information relating to the protection of children or vulnerable adults.

## Data Security

Physical copies of client data are kept in a locked cabinet in the Farm Office accessible only to those staff who have need. The servers at the farm have security updates applied on a weekly basis. The system is protected by a proprietary anti-virus system, which is updated 'live'.

Data kept on computers is stored on the server within operating with Windows Server 2008. The Active Directory system is used to ensure that only authorised staff are included in the security group with access to client data. The server is based on site in a secure room. All servers run the standard Windows firewall and have active monitoring to block and alerts us to intrusion attempts. The system is periodically scanned for unauthorised connected devices. Public wifi is separated from the internal network via mesh devices and cannot be used to access servers or local PCs. Servers are inaccessible from the internet or external networks unless connected via a VPN which is locked down to only specified users through the router using SSL encryption.

Client data is not taken off site in any electronic form. Should transfer of data off site be required it must be encrypted before being written to portable media.

Web-based services used to store client data are vetted to ensure compliance with GDPR requirements. These include FirstSteps (nursery data), MailChimp (mailing lists), Membermojo (memberships).

## Data incidents

When a breach of data security has been suspected, measures will be put in place immediately to prevent any further data loss. An investigation will be undertaken to determine what data may have been compromised. The methodology developed by ENISA (https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport) should be used to determine the scale of the breach.

Where a breach is detected those people whose data has been compromised must be contacted and informed about the nature of the breach. If the breach is a major one then the ICO should be informed within 72 hours of the incident (see https://ico.org.uk/for-organisations/report-a-breach/).

The GDPR imposes a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. A personal data breach means a

breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

## Retention of Data

The Farm will hold the minimum personal data and sensitive personal data necessary to enable it to perform its functions. The retention schedule at Appendix A sets out the length of time that different types of data will be kept. The Farm will keep some items of information for longer than others. The retention period will never be for longer than is necessary and in line with current good practice and statutory requirements.

Records retained will be kept in a secure location. The erasure or destruction of information which is out of date will be conducted in such a way as to preserve the confidentiality of the information. All paper records that contain confidential information will be kept in locked cabinets and the keys will only be available to approved personnel. All confidential electronic data will be stored in restricted locations on the server. Access to these locations will only be for approved personnel decided by the Chief Executive.

# Appendix A - Information Governance

## Retention schedule

| Type of record | Retained for: | Why retained |
|---|---|---|
| Employee information | 7 years from the termination of employment | The purpose for which the Farm holds any information about Employees after the end of employment is for use solely in relation to residual employment related matters including, but not limited to; the provision of job references, processing applications for re-employment, matters relating to retirement benefits the fulfilment of contractual or statutory obligations. |
| Job candidate information | 6 -12 months | The records of unsuccessful job applicants will be kept for 6 months. This allows for revisit if the recruitment is unsuccessful and also for challenge of the recruitment process. |
| Nursery pupil information | 10 years from date of leaving nursery | This information is retained for this period in line with OFSTED and BAND recommendations. This is for the purpose of evidence of any (but not limited to) child protection, health or queries about procedural issues that may arise later in the child's life. |
| Finance records | 7 years | Statutory guidelines |
| Volunteers, clients and service users | 2 years from date of last contact | This will allow for references to be provided (if applicable) and for funding reporting. |
| Volunteer applicant information | 1 year | The information about people who have applied to volunteer but have not been placed will be kept for 1 year to allow placement when possible. |

## Information Governance Improvement Plan

The Information Governance Toolkit (login at https://www.igt.hscic.gov.uk/home.aspx), used by the organisation to check and develop its practices, requires the organisation to have an improvement plan. The status of the various requirements is laid out below. Note that this table may be updated between updates of the policy without the need for re-approval by trustees.

| Requirement | Current Status | Target, next steps | Action |
|---|---|---|---|
| 14-114<br>Staff assigned | Level 3 | Annual review of IG arrangements. | |
| 14-115<br>Policy | Level 2 | Regime of testing compliance required | |
| 14-116<br>Contracts identify IG | Level 2 | Monitoring system required | |
| 14-117<br>Staff training | Level 1 | Documented assessment of training | |
| 14-202<br>Personal info disclosure | Level 3 | Ongoing monitoring | |
| 14-209<br>Overseas transfers | NR | None | |
| 14-213<br>Info leaflet for public | Level 2 | All written coms have note on how to access info. | |

| | | | |
|---|---|---|---|
| 14-214<br>Code of conduct | Level 2 | Spot check compliance | |
| 14-215<br>New processes comply | Level 0 | Documented procedure for identifying new systems | |
| 14-216<br>Confidentiality audit | Level 0 | Develop audit process for confidentiality | |
| 14-304<br>NHS Smartcards | NR | None | |
| 14-316<br>Info asset register | Level 1 | Compile a list of info assets | |
| 14-317<br>Physical access | Level 0 | Risk assessment of unauthorised access | |
| 14-318<br>Mobile systems | NR | None | |
| 14-319<br>Business Continuity | Level 2 | Annual review of business continuity plan needed | |
| 14-320<br>Incident management | Level 2 | Compliance checks need to be set up | |
| 14-321<br>Computer based info | Level 2 | Document how users are assigned permissions (level 1 requirement)<br>Regime of monitoring to be developed. | Steve |
| 14-322<br>Transfer of info | Level 0 | Identify transfers of info<br>Document a procedure | |
| 14-325<br>ICT security | Level 2 | Monitoring & testing regime needed. | |
| 14-412<br>Accuracy of records | NR | No demographic info. | |

## Information flows

This section relates to IG toolkit requirement 14-202 and 14-322

| **Information** | **Basis for holding** |
|---|---|
| Personal information supplied to us by client | Consent of client given |
| Personal information received from referring agency (eg risk assessment ) | Consent of client given in application (references will be sought) |

## Procedure for transferring data

Information sent to us (eg risk assessments) does not identify clients other than by initials. Once risk assessments and references are received (either electronically or in paper format) they are stored along with the clients application form in a locked filing cabinet in the farm office. Clients are informed of this information sharing procedure on the volunteer application form.

This information is never sent out and kept in the secure location for duration of engagement and for a period of 2 years following end date (see Appendix A - Information retention schedule).

### New services

This section relates to IG toolkit requirement 14-215

When new services are introduced to the organisation consideration of their impact on the security of personal information must be considered.

### Audit Requirements

The Health & Social Care Operations Manager will check annually which staff have access to personal information and will assess their level of knowledge about it correct use and protection.

### H&SC information asset register

This section relates to IG toolkit requirement 14-316

| Information | Location | Used by |
|---|---|---|
| Personal information supplied to us by client | Filing cabinet in Farm office | H&SC staff. |
| Personal information supplied to us by client | Excel spread sheet held on server | H&SC staff. |
| Risk assessments supplied by referring agencies | Server (L: H&SC/Risk Management) | H&SC staff. |

## Appendix B – General Data Privacy Notice

### Summary

Windmill Hill City Farm (WHCF) is committed to protecting your personal data and handling it responsibly.

This policy covers the personal data that WHCF collects whenever you interact with us, including and not exclusive to, when you use our website and social media sites, use our facilities (such as the Children and Family services, Health and Social Care Services and , when you attend workshops, events or hire rooms and football pitch), and when you correspond with us such as by email or over the phone. It also covers personal data that we may receive from third parties.

The sections below explain in more detail:

- the types of personal data we collect from you
- the types of personal data we receive from third parties
- why we process your personal data
- who we share your personal data with
- personal data transfers outside of the EEA
- how long we retain your personal data
- your rights to withdraw your consent and to object (including to direct marketing)
- your other personal data rights

- how to contact us and exercise your rights

If you would like to know how we collect information about your use of our websites, social media sites, you please read our Web Privacy Policy.

Personal data WHCF collects from you

This policy covers the personal data that WHCF collects whenever you interact with us, including when you use our facilities such as:

- Children and Family services
- Health and Social Care services
- School and family support services
- when you attend workshops, events or hire rooms and football pitch at WHCF
- when you use our website and social media sites
- Correspond with us (such as by email or over the phone).

The personal data we collect from you may include:

- the name and contact details that you provide when you register as a member, Nursery placement, H&SC placements room hire and football pitch, workshops, events, work placements with us
- your payment and address details
- your marketing preferences, including any consents you have given us
- information about your use of our websites and social media
- your communications with us
- information about your attendance at WHCF events, such as courses, sessional fairs and other activities arranged by WHCF. Photos and video footage of you may be taken at these events

Personal data WHCF receives from third parties

Sometimes we receive personal data from third parties, in particular

- Referral agencies (eg other third sector organisations, hospitals) for health and social care clients.
- Referral agencies (eg local authority) for children and family services

Why WHCF processes your personal data

This section explains the reasons why we process your personal data and our legal bases for doing so.

*Consent*

If you've opted-in to receive information relating to WHCF, then we'll provide this information to you by email, text, or phone. We also rely on your consent to process information about your use of our website and social media sites. Wherever we rely on your consent to process personal data, you have a right to withdraw that consent. See how you can exercise your rights at the end of this document.

*Legitimate interests*

We process your personal data when necessary to pursue our legitimate interests in the following

- tailoring our websites and communications for you. We collect information about your engagement with us online (such as pages that you have visited on our websites or apps) to use for analysis of web traffic
- monitoring, improving and protecting our content and services
- sending you some types of direct marketing, including by email and post
- responding to your comments or complaints
- undertaking, or inviting you to take part in, market research
- preventing, investigating and/or reporting fraud, terrorism, misrepresentation, security incidents or crime
- using incident reports and CCTV footage to protect the security of our visitors and staff and to help detect and prevent unlawful activity
- managing legal claims, compliance, regulatory and investigative matters
- processing job applications received through www.windmillhillcityfarm.org.uk or info@windmillhillcityfarm.org.uk

You have a right to object to any processing that we undertake for our legitimate interests.

*Contract*

We process your personal data when we are administering your involvement in services (eg Children and Family Services, Health and Social Care activity, Schools and Family activities.

*Legal obligation*

We are legally required to process your personal data in cases where we need to:

- obtain parental consent to provide services directly to children
- respond to certain requests by government or local authorities

Who WHCF shares personal data with

We will share your personal data with the following recipients.

- Police or other agents of the state where we are required to do so by law
- Care teams with whom you have an existing relationship (eg organisations that have referred you to us)

Personal data transfers outside of the EEA

No data is transferred outside the European Economic Area

How long WHCF retains personal data

We retain personal data for as long as your account remains active, and for a limited period of time afterwards (in case you decide to reactivate your membership or have queries about it).

We retain personal data relating to your purchases for several years from the date of the relevant transaction. This is to understand your purchasing preferences and to meet our legal and contractual obligations.

Where you have asked us not to send you direct marketing, we keep a record of that fact to ensure we respect your request in future.

We also retain information with the potential to give rise to legal disputes for 7 years.

Your rights to withdraw consent and to object (including to direct marketing)

Wherever we rely on your consent to process personal data, you always have a right to withdraw that consent. You also have the right to object to any use of your personal data for direct marketing purposes, as well as to processing that we undertake based on our legitimate interests (including profiling).

Your other personal data rights

In addition to your rights to withdraw your consent and to object, you have the right to ask us:

- for access to information about your personal data or for a copy of your personal data
- to correct or delete your personal data
- to restrict (i.e. stop any active) processing of your personal data
- to provide you with certain personal data in a structured, machine readable format and to transmit that data to another organisation

These rights may not always apply, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have a compelling legitimate interest in keeping. If this is the case then we'll let you know when we respond to your request.

How to contact us and exercise your rights

The easiest way to stop receiving information from us is by opting out of communications through emailing info@windmillhillcityfarm.org.uk

We will do our best to assist with any queries you have about your personal data. You can contact our Data Protection Officer at any time using the contact details below. When you do so, please provide your full name, your preferred contact information, and a summary of your query.

Data Protection Officer

Windmill Hill City Farm Ltd.

Philip Street

Bedminster

Bristol

BS3 4EA

If you have unresolved concerns, you also have the right to complain to an EU data protection authority where you live, work or where you believe a breach may have occurred. This is the Information Commissioner's Office in the UK.

# Appendix C – Internal communication approach

## Background

Communication is fundamental to the success of the organisation. It is key to achieving our aim to 'support, develop and value high quality staff' and in engaging them in the strategic direction of the organisation. This section outlines the responsibilities of staff in maintaining good communication practice, the main communication channels available and how they might be used to be effective.

It refers primarily to communications within the organisation and aims to ensure staff are informed of relevant activity; are effective in their role; maintain good communication practice and have effective methods of communicating during a serious incident.

## Responsibilities

All staff must play an active role in ensuring internal communications are successful. Department heads and managers need to ensure appropriate information is available to staff in a timely manner and should maintain open channels of two-way communication and to listen to feedback from their teams.

All staff need to be active in seeking the information they need so as to be as effective as possible in their role and to support the strategic direction of the organisation.

## Communication channels

The range and use of communication channels available is rapidly changing. This section acts as guidance on the limitations of current channels.

### Face-to-face communication

Communicating in person with colleagues is an effective method of ensuring information and knowledge are shared. The conversational nature allows for greater understanding of the context of the message and encourages questioning and feedback. There are some circumstances where face-to-face communication is required, eg in performance management procedures.

### Email

All staff are issued with a 'company' email address in the form *firstname.surname*@windmillhillcityfarm.org.uk. This address gives access to the Microsoft Teams environment as well as being the address to use for work-related messages.

Email Conduct

- Email messages that are created, sent or received using the organisation's equipment are the property of the organisation
- Global e-mails should not be used for personal issues (ie not work-related).
- E-mail messages should be treated as permanent written records which may be read by other people and which could result in personal or organisation liability.
- Employees should not:
  - Assume because an email has been sent that it has been read or acted upon.
  - Retrieve or read email messages that were not sent to them

  - Impersonate any other person when using email
  - Use email to send defamatory messages that criticise other individuals or organisations.
  - Send or distribute e-mail messages which are abusive, defamatory, pornographic in nature or make any improper or discriminatory reference to a person.
  - Copy, download or forward to third parties, via e-mail, the work of other people protected under copyright, without their consent.
  - Create email congestion by sending trivial messages eg chain mail letters, humorous stories.
- Incidental and occasional personal use of email is permitted. Such messages become the property of the organisation and are subject to the same conditions as organisation email messages.
- Employees should be aware of phishing and other malicious messages and delete suspicious traffic. In case of doubt contact a manager or IT support directly.

Where email is used for bulk mailing, software specific to that purpose should be used (eg MailChimp). Outlook is not well suited to bulk mailings: it has in-built safeguards that shut down accounts that send to multiple addresses frequently; spam filters often block messages blind copied to multiple addresses (meaning messages may not arrive); and there is a significant risk that multiple email addresses will be exposed to recipients (which may constitute a data breach).

## Social media

Social media sites such as Facebook, Twitter or Instagram are part of the external communications used to promote the organisation. They should not be used between colleagues for work-related communication.

The organisation does not, and cannot control the use of social media between colleagues in a personal (social) capacity. However, it should be noted that when staff make reference to colleagues or the organisation within their personal communications (by whatever means) they are still subject to the organisations policies, in particular regarding confidentiality (of company or client information) and respect and dignity. Sanctions may be brought against staff contravening these policies on social media channels.

## Messaging services

There is a diverse and growing range of messaging services now available (eg WhatsApp, Slack). These offer the advantage of mobile connectivity to personal devices and ease of use. The disadvantages to them for the organisation are two-fold:

- The expectation that staff use and are asked to share personal phone numbers to facilitate work communication may contravene GDPR rules and constitute an unwelcome intrusion into their home life.
- The organisation has little-to-no control over the data that is exchanged over these services meaning that data it is responsible for has effectively left the organisation.

The organisation uses Microsoft Teams as its preferred messaging service, using a work-provided email address as the identifier. It should be used for all messages shared with work groups.

The use of individual staff phone numbers should be limited to messages personal to them, with due consideration given to the timing of calls and messages (eg not calling during home or holiday time unless the message is urgent).

Like social media sites, the organisation does not, and cannot, control the use of messaging services between colleagues for social purposes, however confidentiality, respect and personal dignity policies may still be applied to messages between colleagues.

### Notice boards

There are notice boards in the staff rooms and in the administration office displaying information for staff. Staff with responsibility for the maintenance of notice boards in their department should ensure that information is advertised in a timely manner and is removed when out of date.

### Professionalism in communication

In all communications staff should serve the interests of the organisation and ensure appropriate content. Staff should ensure appropriate response times are adhered to when communicating, particularly via email. During absence or when staff will not be able to respond in a reasonable time, staff should provide an autoreply to their emails with details of an alternative contact.

### Related policies

This approach should be read in conjunction with the following documents:

- GN01 Employee Handbook
- GN06 Equality & Diversity policy
- GN29 Respect & personal dignity policy
- GN36 Incident and Emergency Guidance

All these policies are available at L:/HR/Public/policies. There are hard copies available in staff areas for reference.

### Further information

The following are circulated to all staff.

- Organisation strategy, developed every 3 years.
- Staff bulletin, produced every 6 weeks.
- Payroll information sheet, produced monthly, focuses on HR matters and information from the Office Manager.

The following are regular meetings.

- Staff meetings – various depending on department but a minimum of once a month.
- General staff meeting – held every 6 months for all staff.
- Staff training day – once a year and is for all staff.

## Appendix D – guidance on IT use

### Introduction

The computer systems of the organisation are essential for its business. Each employee should see helping to safeguard these systems as a fundamental part of their job. This includes avoiding risks such as

introducing unauthorised software, complying with copyright and data protection laws, and being careful to protect the security of sensitive information.

This document outlines the procedures and employee responsibilities when accessing the Internet, sending and receiving emails and using the organisation's computer systems. The organisation views misuse of computers as serious misconduct which could, depending on the circumstances, result in dismissal. Misuse amounting to criminal conduct will be reported to the relevant authorities. The policy should be read in conjunction with GN34 Communication Policy, in particular with regard to social media.

Reference to 'computers' in this document includes desktop and laptop computers, tablets and telephones.

## General

- Only software approved and licenced by the organisation, and approved data are allowed on the organisation's computers.
- Employees are only allowed access to those parts of the computer system which they need to carry out their normal duties.
- Employees must comply with local procedures to ensure that software is virus-free.
- Employees must adhere to the Information Sharing and Confidentiality (Data Protection) policy.
- Employees must observe the Computer Misuse Act 1990, in connection with both the organisation and third parties.
- Passwords must be used at all times and changed regularly; avoidance of obvious passwords is essential. Employees are responsible for the security of their own passwords and workstations.
- Computer game playing is not permitted whilst in a work environment.
- The downloading, transmission or storage (including streaming) of music or video for personal use is prohibited.
- Use of any organisation systems including email and the internet to conduct private or freelance business for the purpose of commercial gain is not acceptable.

## Data processing

The General Data Protection Regulation sets down limits around how personal data can be processed. Staff should ensure that any use of email to send out information to groups of recipients is compliant with this regulation. In broad terms recipients need to have opted in to receive the specific type (topic) of message being sent.

It should be clear when people sign up to receive news and updates from us how their data will be stored, to what use it will be put and what rights they have to be removed from future mailings.

## Internet Usage

- The use of the Internet for personal matters is permitted if the use is incidental, occasional and outside working time. Inappropriate or excessive use of the internet for personal reasons may result in disciplinary action and/or removal of the facility.
- Internet sites visited must not contain content that may be considered illegal, offensive or disruptive. Offensive content includes but is not limited to pornographic, obscene or harassing language or images, racial, ethnic, sexual or gender specific comments or images.

- An employee must not distribute confidential, proprietary, and/or sensitive corporate information to external Internet sites or users without the appropriate authority.
- The organisation retains the right to block access to any Internet site they deem may contain inappropriate material.

## Monitoring

- The organisation recognises that employees have a legitimate expectation that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment. However the organisation reserves the right to monitor employee email or internet activity where it is necessary to prevent or detect;
  - Unauthorised use of the organisation's computer systems
  - Criminal activity including but not limited to fraud, harassment and obscenity
  - Detrimental impact upon the efficient operation of organisation systems
  - Breach of regulatory guidelines
  - Excessive personal use of the internet or email-system.
  - Breach of the organisation's policies
- The organisation has the ability and legal right to monitor e-mail usage and internet usage. By using e-mail and internet the employee consents to any monitoring the organisation considers justified to achieve one of the above aims or to protect any other legitimate interest.
- When the monitoring of personal e-mails is necessary monitoring will be confined to the message address or heading.
- Covert monitoring will only be performed in exceptional circumstances and only when sanctioned by the Chief Executive.
- If information gathered from monitoring may have an adverse impact on an employee, it will be presented to them and they will be allowed to make representations before any action is taken.
- Information gathered through monitoring will only be used for the purpose for which the monitoring was carried out, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore.
- All information gathered through monitoring will be held securely and kept for no longer than is necessary to achieve the aim for which it was collected.
- The Data Protection Act 1998 allows employees to have access to information stored about them. You can ask for access to your own personal details held on computer or held manually. If you wish to see your records, you should give the Farm notice in writing and it may take up to 1 month to provide the information .

## Disclosure

- All employees have a duty to report the following to their line manager:
  - suspect e-mails/e-mail attachments
  - obscene or illegal material found on a PC or sent via email
  - persistent use of the internet or email system for personal reasons
  - downloading of illegal/obscene/offensive material.