FUN 4 YOUNG PEOPLE

Fun 4 Young People

Information and Assets Governance Handbook

Contents

Policy Family	Policy No.	Policy	Policy Owner
1.3 Information and Assets Governance	1.3.1	Data Protection Policy	Trustee
1.3 Information and Assets Governance	1.3.2	IT and Social Media Policy	CEO
1.3 Information and Assets Governance	1.3.3	Client Privacy Notice	Trustee
1.3 Information and Assets Governance	1.3.7	Employee Privacy Notice	Trustee
1.3 Information and Assets Governance	1.3.4	Communications Policy	Trustee
1.3 Information and Assets Governance	1.3.5	Safeguarding Assets Policy	Trustee

INTRODUCTION

Established as a registered charity in March 2022, Fun 4 Young People (F4YP) Ltd. (F4YP) are an equal opportunities employer and do not discriminate on the grounds of gender, sexual orientation, marital or civil partner status, pregnancy or maternity, gender reassignment, race, colour, nationality, ethnic or national origin, religion or belief, disability or age.

The policies in this Handbook are designed to ensure that we fulfil our obligations under applicable laws to service users, participants, stakeholders and otherwise to protect the interests of those members of society who may be vulnerable to risks identified in applicable legislation.

The policies and procedures set out in this handbook apply to all personnel unless otherwise indicated. Personnel includes employees, casual and sessional contractors, volunteers and trustees, as well as all other persons supporting, providing, or delivering services for or on behalf of F4YP. They do not form part of the terms of your contract with us, which are provided to you separately.

DATA PROTECTION POLICY

Policy Statement

The following policy sets out the framework for the collection, processing and security of data needed to deliver our services, which is designed to achieve a high level of protection for Fun 4 Young People (F4YP) Ltd. (F4YP) and its service users.

Scope

This policy applies to: -

- All personnel this includes employees, casual and sessional contractors, volunteers and trustees, as well as all other persons supporting, providing, or delivering services for or on behalf of F4YP
- Parent/carer/guardian and service users.

Introduction

It is necessary for F4YP to hold personal data about its Personnel, Service Users, Service User families/guardians and Providers to enable the organisation to respond to and meet service needs. It is vital that Personnel who collect and use personal data comply with the requirements of the Data Protection Act 2018 and the UK GDPR.

Personnel who collect personal information must inform the individual of the purpose for which the data is being collected, which is detailed in our Privacy Notice. Once collected, this data must not be disclosed to a third party without a lawful basis, except where legally obliged to do so.

F4YP is registered with the ICO under the Data Protection Act 2018 and fully committed to compliance with the requirements of the UK GDPR, (henceforth referred to as "the Acts") and abides by their provisions. F4YP will therefore follow procedures that aim to ensure that all Personnel (Employees, Trustees, contractors, volunteers) have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the Acts.

Informing Service users about Confidentiality Standards

Service users are informed that any information held is treated as confidential, stored in a secure manner and accessed only by F4YP staff, volunteers and agreed partners. Service users are to be informed how the information gathered may be used and what their rights are in respect of their data via F4YP's Privacy Notice.

- There are certain exceptions to the above such as in cases where there is clear evidence of serious risk to an individual or to the welfare of others. No guarantee of confidentiality will be given in the following circumstances:
- Where child protection/vulnerable adult issues are involved
- Where there is significant threat to life
- Where a Service users' needs urgent medical treatment
- Where information regarding a criminal offence is disclosed
- Where a breach of a statutory provision is concerned

Service user Permission to Disclose Information

A service user has the right to expect that information given in confidence will be used only for the purpose for which it was given and that it will not be disclosed to others without permission unless there is an overriding obligation or duty to pass on that information. Explicit permission should always be sought and appropriately logged when the service user subscribes for the service. If a service user has a language difficulty the implications of obtaining the consent will be clearly explained. If required a translation service will be used. It must be emphasised to service users that only relevant information will be passed on.

F4YP Personnel will ensure that Service users understand that the information is available to F4YP Personnel for the purposes of providing our services to them.

Confidentiality and Recorded Information

Information collected and recorded should:

- reflect the needs of the service user
- be as up to date and accurate as possible
- be factual information about what was discussed along with any relevant implications and is as free as possible from any bias
- should be non-judgemental
- avoid stating opinions unless evidence exists to support it
- be relevant
- be recorded concisely and legibly, using appropriate language
- be initialled and dated either physically or digitally
- be, where possible, agreed with the service user.

In recording information gained from third parties it is made clear from whom the information has been obtained.

Storage of Records and Access

Information relating to service users is held confidentially and is stored securely on a secure IT system.

Personnel must ensure when information is in use that it is not accessible to third parties by:

- not leaving written information unsecured where it could be read by others

- ensuring that information on electronic devices is not visible to others and such devices are 'screen locked' when not in use or unattended
- ensuring individually identifiable information held on computer is protected from inappropriate access by use of access passwords
- not discussing information relating to a Service User within the hearing of others who should not have access to this information
- Access to Service User's records is restricted to F4YP staff (and, where appropriate, agreed partners & volunteers) in order to carry out their duties.

Personnel will only access individual Service User records when they have a legitimate purpose for doing so. Examples of legitimate purposes are in order to provide services to service users, or for staff development in relation to use of the system.

A Service User, current or former, asking to see their file or items contained within it should be referred to the Data Protection Officer (dpo@f4yp.org) and the request will be handled as a Subject Access Request in line with the Acts.

Implementation

It is the role of F4YP's Board to determine policy considering legal requirements. The Board is also responsible for ensuring that information governance is adequately resourced.

- The Chief Executive will have overall responsibility for ensuring that this policy is implemented.
- The Data Protection Officer (contactable on dpo@f4yp.org) has responsibility for:
- Undertaking risk assessments and taking steps to ensure that risks are mitigated, reporting to the CEO & Board as necessary
- The provision of data protection training, for staff in conjunction with the HR function
- The development of practice guidelines and procedures
- Carrying out compliance checks to ensure adherence to the Acts and this policy
- Developing information sharing protocols between the component member organisations within F4YP
- Any necessary recording and reporting of incidents breaching the Acts and/or this policy to the ICO

IT AND SOCIAL MEDIA POLICY

Policy Statement

This policy covers all forms of IT & social media, including Facebook, LinkedIn, Twitter, Google+ Wikipedia, other social networking sites, and other internet postings, including blogs. It applies to the use of devices, systems and software relating to F4YP. It also applies to use of social media for both organisation and personal purposes, during working hours and in an employee's own time to the extent that it may affect the business of Fun 4 Young People (F4YP) Ltd. (F4YP). The policy applies both when social media is accessed using F4YP devices and when access using equipment or software belonging to employees or others.

Scope

This policy applies to: -

- All personnel this includes employees, casual and sessional contractors, volunteers and trustees, as well as all other persons supporting, providing, or delivering services for or on behalf of F4YP

Introduction

Whilst we recognise the benefits which may be gained from appropriate use of IT & social media, it is also important to be aware that it poses significant risks to F4YP. These risks include disclosure of confidential information and intellectual property, damage to our reputation and the risk of legal claims. To minimise these risks this policy sets out the rules applying to the use of IT and social media.

This policy covers all personnel. Breach of this policy may result in disciplinary action up to and including dismissal. Any misuse of social media should be reported to the Chief Executive Officer.

IT Equipment

Mobile phones/laptops or tablets may be allocated to staff on a business needs basis and by agreement with senior management. Any allocation may be given on either a permanent basis for regular use in connection with their work or on an ad hoc basis as required from a "pool" of equipment.

If you are issued with any IT equipment, you are responsible for its security whilst it is allocated to you. It always remains the property of the Organisation and shall be returned to the Organisation should you leave its employ, or it is deemed no longer a requirement of your job, together with any issued accessories or devices.

In accordance with legislation, you may not use handheld mobile phones or similar device(s) whilst operating machinery or driving unless your car is fitted with suitable hands-free equipment and allows you to make and receive calls in accordance with legal requirements.

Work devices must be password or PIN protected.

Passwords

Personnel shall be responsible for password protecting and locking their laptops, tablets and mobile phones. Personnel shall not disclose passwords to another person or allow them to be used, unless the other person is an administrator of our IT systems. F4YP mobile phones and tablet pins can be disclosed to F4YP team.

Responsibility

The user is responsible for the care of the equipment at all times so that it is kept in a good working condition. Any damage or theft/loss should be reported immediately to F4YP. The equipment itself must be PIN code or password protected to minimise security risks. If equipment is broken or faulty then it should be returned to F4YP. Depending on the circumstances in which the equipment is faulty or broken, F4YP will be responsible for replacing it. However, if carelessness on the part of the user can be shown, the user will be required to meet the replacement cost.

Emails and Online Calendars

Work email accounts are the property of the Organisation and may be accessed by the organisation at any time and for any reason. Use of email by Personnel is permitted and encouraged where such use supports the goals and objectives of the business. Personnel must ensure that they:

- comply with current legislation including the Data Protection Act 1998
- use email in an acceptable way
- do not create unnecessary business risk to F4YP
- do not use F4YP email domains for personal business use
- do not distribute, disseminate or store images, text or materials that might be considered indecent, pornographic, obscene or illegal
- transmit unsolicited commercial or advertising material
- do not knowingly introduce any form of computer virus or malware into the corporate network

F4YP reserves the right to investigate any potential wrongdoing. This may include searching any work emails, devices or systems.

Personal calls

F4YP recognises that employees may have to make personal calls during working hours or outside normal working hours. Where it is deemed that an unreasonable level of personal calls/text messages/data usage is being made the disciplinary procedure may be followed.

Use of social media at work

We allow staff to make occasional personal use of social media so long as it does not involve unprofessional or inappropriate content and does not adversely affect your productivity or otherwise interfere with your duties to us. Any use must comply with this policy. We may monitor your use of its systems, including use of internet and social media sites.

Personnel should only access their personal social media accounts their own devices.

If you are required or permitted to use social media sites while performing your duties for or on behalf of F4YP you should ensure that such use has appropriate authorisation and that it complies with the standards set out in this policy.

Responsible use of social media

You must not use social media in a way that might breach any of our policies, any express or implied contractual obligations, legislation, or regulatory requirements. This includes both work and personal use of social media or associated accounts.

Use of social media must comply with:
• the Equality, Diversity and Inclusion and Anti-Bullying and Anti-Harassment, Policies
• rules of relevant regulatory bodies
• contractual confidentiality requirements
• other key policies/requirements.

Use of social media must not:

- contain disparaging or defamatory statements about F4YP, our personnel, service users or partners
- harass, bully or unlawfully discriminate in any way
- use data obtained in the course of your employment with F4YP in any way which breaches the provisions of the Data Protection Act 1998
- breach copyright belonging to us
- disclose any intellectual property, confidential or commercially sensitive information relating to F4YP
- make statements which cause, or may cause, harm to our reputation or otherwise be prejudicial to our interests.

F4YP recognises that many Personnel make use of social media in a personal capacity. While they are not acting on behalf of F4YP, they must be aware that they can damage F4YP if they are recognised as being one of our Personnel. You should avoid using social media communications that might be misconstrued in a way that could damage our reputation.

Personnel are allowed to say that they work/volunteer for F4YP, which recognises that it is natural for its staff sometimes to want to discuss their work on social media. However, the Personnel's online profile (for example, the name of a blog or a Twitter name) must not contain F4YP's name. It is advised by F4YP that all personal social media profiles are made private and secure so that service users cannot access their information. We also ask that you declare any previous relationships with service users and that you do not accept any requests to follow your personal social media from accounts from our service users.

You should make it clear in personal postings that you are speaking on your own behalf, in particular write in the first person and use a personal e-mail address. If you disclose that you are an employee of us, you must state that your views do not represent those of your employer. For example, you could state, “the views in this posting are my own and do not represent the views of F4YP”

Remember that you are personally responsible for what you communicate in social media. Often materials published will be widely accessible by the public and will remain accessible for a long time. If you are uncertain or concerned about the appropriateness of any statement or posting, you should discuss it with your manager before making the post.

The contact details of business contacts made during your employment are regarded as confidential information belonging to F4YP. On termination of your employment, you must provide us with a copy of all such information and destroy any further copies of such information that you may have.

Where it is believed that an employee has failed to comply with the terms set out in this policy the disciplinary procedure should be followed.

CLIENT PRIVACY NOTICE

Policy Statement

The following policy sets out the type of data we need to collect and process in order to deliver our services to you. Both policy and practice are designed to achieve a high level of protection for Fun 4 Young People (F4YP) Ltd. (F4YP) and you, its service users.

Scope

This policy applies to: -

- All personnel including employees, casual and sessional contractors, volunteers and trustees, as well as all other persons supporting, providing, or delivering services for or on behalf of F4YP
- Service users including young people, their parents/carers/guardians and close family.

The type of personal information we collect

We hold some personal information about you/your young person/family to make sure we can help and look after you/your young person/family at F4YP services & events.

This information includes:

- Contact details
- booking/attendance records
- characteristics, such as ethnic background or any special educational needs
- Any medical conditions
- Details of any behaviour challenges
- Details of bursary criteria
- Details of who lives in your family home
- Details of other professionals working with you/your family/your young person, for example schools or social services.
- Records of professional/ multi-agency meetings

How we get peronal information and why we have it

Most of the personal information we process is provided to us directly by you/your young person, and is processed for one of the following reasons:

- Getting in touch with you and your young person when we need to
- To safeguard you/your young person
- Looking after you/your young person's wellbeing and to support you/your young person
- To provide ongoing pastoral support
- To track attendance
- To create anonymous statistics for funding

For the same reasons, we get information about you/your young person from some other places too;

- Schools
- Social Services if applicable
- Other agencies supporting you
- Our providers (see below)

Who we share information with and why

Below we have listed types of organisations we share data with, what sort of data and the legal basis under General Data Protection Regulation (GDPR) for sharing it (see the ICO website for further information)

Third Party Activity Providers

We share the relevant information we hold with our provider organisations for them to deliver their services as part of our activity programmes.

Providers include:
Canoe Trail
Spiral Freerun
Sophie Ibbott Therapy

Legal basis for this sharing: Contract (personal information we need to provide our service to you/your young person safely)

Funders

We share anonymised statistics to funders as part of our contract with them

Legal basis for this sharing: Legal obligation (anonymised statistical information - see the ICO website for further information)

We may also share images and/or case studies of you/your young person/family to provider organisations, funders and/or via social media and our website if you have given us consent to do so. We ask for your consent on our booking forms (www.f4yp.eventbrite.co.uk). You can withdraw your consent at any time with no impact upon the service we are able to provide to your / your young person/family. However, we may not be able to remove any/all images or case studies used prior to consent being withdrawn.

Legal basis for this sharing: Your consent (photos, case studies, some personal information)

Funders include:
The National Lottery Community Fund
Bedford Borough Council
Harpur Trust
Bedford Giving
Children In Need
Carlton Educational Trust
Co-Op Community Fund

Garfield Weston Foundation
John Laing Foundation
Kerslake Robshaw Foundation
Mazars
Wixamtree Trust
Gale Family Trust
GT Railway
Masonic Charitable Foundation
Sport England
BLCF
Bedfordshire Charitable Trust
Foyle Foundation
(last updated April 2025)

Statutory Services & other supporting agencies
This primarily relates to schools / statutory education providers but could also home education services, emergency health services, other local government departments such as social services or housing and other support services working with you, your young person or your family.

Schools, statutory education & home education providers
As part of our pastoral support, we provide termly reports to each young person's school which includes an overview of their progress; support needs identified at club(s) and attendance information. We may also discuss pastoral support in relation to your young person between times of reports.
Legal basis for this sharing: Contract (personal information we need to provide our service to your young person safely)

Emergency health services and local government departments such as social services or housing
We may share information with such providers when we believe it could pertain to safeguarding someone.
Legal basis for this sharing: Legal obligation (information which we believe could pertain to safeguarding someone – see our Safeguarding Policy and the ICO website for further information)

Other supporting agencies
We may share information with such providers when we believe it could pertain to safeguarding someone, or where you have given your consent for us to share information in order for both services to better support you, your young person or your family.
Legal bases for this sharing:

- Legal obligation (information which we believe could pertain to safeguarding someone – see our Safeguarding Policy and the ICO website for further information)
- Your consent (personal information related to support needs but not safeguarding)

How we store your personal information

Your information is securely stored on Eventbrite and Salesforce cloud-based servers.
How long we retain your data depends on how old you were when you first came to F4YP.

Under 18 at first contact

We keep the personal information we collect until the Service Users 25th Birthday unless records contain positive handling incident records, in which case records are retained until the Service User's 85th Birthday. When we dispose of Service User information, it is deleted and purged from all systems.

Over 18 at first contact

We keep the personal information we collect until 7 years after the Service User leaves our service, unless;

- records contain positive handling incident records, in which case records are retained until the Service User's 85th Birthday.
- The information specifically relates to another Service User who was under 18 at first contact (see above retention periods)

When we dispose of Service User information, it is deleted and purged from all systems.

Your data protection rights

Under data protection law, you have rights including:
Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please see the ICO website for further information on your rights, and contact us at dpo@f4yp.org if you wish to make a request.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at dpo@f4yp.org

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Our registered ICO number is: ZB315189
Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

EMPLOYEE PRIVACY NOTICE

The Charity is aware of its obligations under the General Data Protection Regulation (GDPR) and domestic data protection legislation and is committed to processing your data securely and transparently. This privacy notice sets out, in line with current data protection obligations, the types of data that we hold about you as an employee of the Charity. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This notice applies to current and former employees, workers and volunteers.

Data controller details

The Charity is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows: Fun 4 Young People (F4YP) Ltd, Rooms 9 & 10 Dombey Court, Pilgrim Centre, Brickhill Drive, Bedford, MK41 7PZ.

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

Types of data we process

We hold many types of data about you, which may include:

- personal details including your name, address, date of birth, email address, phone numbers
- Head shot photograph
- gender
- marital status
- dependants, next of kin and their contact numbers
- medical or health information including whether or not you have a disability and details of any disability
- information used for equal opportunities monitoring about your sexual orientation, religion or belief and ethnic origin
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK
- driving licence
- bank details
- tax codes
- National Insurance number
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment/engagement with us

- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings or, in the case of workers, confirmation of other discussions about your conduct
- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms or, in the case of workers, confirmation of other discussions about your performance
- leave records including annual leave, family leave, sickness absence etc
- details of your criminal record
- training details
- CCTV footage
- building entry card records.

How we collect your data

We collect data about you in a variety of ways, and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment/engagement, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as but not limited to employment agencies or former employers when gathering references, training providers for external training.

Personal data is kept in personnel files or within the Charity's HR and IT systems.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment, volunteer or services contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- to protect your interests
- where something is done in the public interest
- where we have obtained your consent.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- carry out the contract that we have entered into with you and
- ensure you are paid or have your expenses reimbursed

We also need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid

- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for individuals with a disability

We also collect data so that we can carry out activities which are in the legitimate interests of the Charity. We have set these out below:

- making decisions about who to offer initial employment/engagement to, and subsequent internal appointments, promotions etc
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- if you are an employee, gaining expert medical opinion when making decisions about your fitness for work
- if you are an employee, managing statutory leave and pay systems such as maternity leave and pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access

Special categories of data
Special categories of data are data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when one of the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations

- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- in our sickness absence management procedures
- to determine reasonable adjustments

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage; however, it may also be collected during your employment where relevant to your continued suitability for your role.

We use criminal conviction data in the following ways:

- To assess your suitability for roles involving contact with children or vulnerable individuals.
- To comply with safeguarding requirements and our legal obligations as a registered charity.
- To carry out Disclosure and Barring Service (DBS) checks where appropriate.
- To ensure we are meeting our duty of care to service users and staff.

We process this data because of our legal obligation to comply with safeguarding laws, including the Children Act 1989 and 2004, the Safeguarding Vulnerable Groups Act 2006, and associated statutory guidance.

We also rely on the lawful basis of substantial public interest, specifically under Schedule 1, Part 2 of the Data Protection Act 2018 (safeguarding of children and individuals at risk), to process this data.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract with us. If you do not provide us with the data needed to do this, we will be unable to perform those duties e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment/engagement with us in relation to our legal obligations if you do not provide us with this information e.g. confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

Sharing your data

Your data will be shared with colleagues within the Charity where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management

of you, the HR Consultant for support and advice and the payroll department for administering payment under your contract.

We may share your personal data with third parties where it is necessary to administer the working relationship, fulfil our legal obligations, or support the effective running of our organisation. These may include:

- Payroll providers – to process salary, tax, and statutory payments.
- Pension providers – to manage your workplace pension scheme.
- External HR consultant (JT HRConsultancy Ltd) – to support HR administration, advice, and compliance.
- Occupational Health providers – for medical assessments and workplace adjustments.
- Disclosure and Barring Service (DBS) – for safeguarding checks where appropriate.
- IT service providers – who support our secure systems and data storage.
- Training providers – for compliance and development purposes.
- Regulatory bodies or law enforcement – where required by law or safeguarding duties.

All third-party providers are required to handle your data in accordance with data protection legislation and under appropriate confidentiality and security arrangements.

We may also share your data with third parties as part of a Charity TUPE or restructure, or for other reasons to comply with a legal obligation upon us.

We do not share your data with bodies outside of the European Economic Area.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. This can be found in the Information and Assets Governance handbook.

Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with current data protection requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

We retain your personal data only for as long as is necessary to fulfil the purposes for which it was collected, including satisfying any legal, accounting, or reporting requirements. Retention periods vary depending on the type of data but are generally in line with our HR Data Retention Policy. For example, we typically retain employee records for 6 years after the end of employment and payroll data for 6 years in accordance with HMRC requirements.

Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold about you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our subject access request policy which is available from *[insert details]*
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact dpo@f4yp.org.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner's Office (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

Data Protection Officer

The Charity's Data Protection Officer is Becky Ireland. She can be contacted at dpo@f4yp.org

COMMUNICATIONS POLICY

Policy Statement

To ensure consistent, effective and appropriate communications – both external and internal – for the organisation to achieve its aims, objectives and policies, and to its credibility as a publicly accountable organisation.

To reduce the risk to the organisation of damaging or ineffective communication, and to ensure that all personnel are aware of how communications are best conducted externally and internally, and who has responsibility for which aspects.

Scope

This policy applies to:

- All personnel this includes employees, casual and sessional contractors, volunteers and trustees, as well as all other persons supporting, providing, or delivering services for or on behalf of F4YP

Introduction

Effective communications play a positive role in the day-to-day operations of the organisation through the consideration of content, and the audience for any particular message or information to be disseminated. Managers and staff at all levels have a responsibility to foster good communications internally and externally.

F4YP aims to foster a culture which encourages transparency of communication, clarity of style and the sharing of best practice and expertise across the organisation

Internal Communications

Include all the messages and information (whether verbal or written) shared within the organisation, principally between all employees, but also between trustees and employees, and to and from management and personnel. Internal Communications include the information given to providers and volunteers.

External Communications

Include all the messages and information that the organisation presents to different audiences, whether directly (through telephone calls, letters, e-mails, newsletters, marketing materials, social media channels, online and press releases) or indirectly through the media and word of mouth. They also include the messages and information given to service users of the organisation, as well as to other stakeholders including trustees, funders, sponsors, supporters and suppliers.

All Communications are important and need to be considered carefully.

Procedure

F4YP will endeavour to do the following to promote effective communication within the organisation:

- promote transparent and open communication
- promote the aims and values of the organisation
- create a trusting working environment in which personnel can locate the information they require
- provide everyone with the skills to be confident communicators
- external and internal communications form part of strategic and business planning, as well as project and team appraisals (including work with other organisations).

All communications should be consistent with the organisation's brand guidelines. These offer guidance on the principles and standards for external communication and define the values and the associated design style to be adopted in all external communications.

Internal Communications

Internal communications are based on active management across the organisation to ensure that:

- Trustees and personnel are informed of the most important relevant information relating to the organisation on a regular basis
- regular exchanges through e-mail, meetings and telephone calls are thoughtful, respectful, efficient, and well disciplined
- staff are asked for feedback on a regular basis about the efficacy of internal communications

External Communications

Corporate and marketing communications should be:

- Approved by the CEO, Head of Operations prior to release/sending.
- Using language consistent with the branding guidelines and F4YP website and policies
- Checked for consent of usage where applicable for example when using the image of a service user, quote of service user/parent/guardian/case study

Responsibilities

Trustees

The Chair of Trustees is responsible for ensuring that the Trustees help to promote the organisation's reputation through consistent external communication.

All Trustees are expected to be familiar with the programmes and activities of the organisation and to refer complex or difficult external questions to the CEO.

Chief Executive Officer

The CEO, with the Head of operations as appropriate, is responsible for the overall clarity and coherence of the organisation's external communications. They will seek opportunities for good advocacy in order to promote the interests of the organisation. The CEO works to create an internal culture of open, honest, efficient and transparent communications.

The CEO will:

- oversee all print communication from the organisation (other than publications) including marketing, social media, development, learning and access, hand lists and signage, as well as setting the standard for communications through the website
- promote effective communications through the media, whether printed or broadcast, and seek collaboration with appropriate media channels
- ensure that communication for visitors within the organisation, and at associated sites, is appropriate and as clear as possible
- work with the Head of Operations to promote good internal and external communications

The Head of Operations will:

- work together with the CEO to act as the public voice of the organisation and communicate with a variety of audiences via a range of media.
- aim to develop an accurate and positive understanding of the organisation's brand and work, and to maintain the organisation's reputation

Personnel

All personnel are responsible for maintaining good internal and external communications, for suggesting improvements wherever possible and for reporting breaches of the policy.

Breach of the Policy

Any actions taken by F4YP personnel which contravene the Communications Policy will be subject to the Disciplinary and Poor Performance policy.

SAFEGUARDING ASSETS POLICY

Policy Statement

This policy outlines the approach to its management of physical, IT and information assets including responsibilities to ensure objectives are met, including safeguarding information from security threats that could have an adverse effect on it operations or reputation, to fulfil the charities duty of care towards the assets to which its been entrusted.

Scope

This policy applies to: -

- All personnel this includes employees, casual and sessional contractors, volunteers and trustees, as well as all other persons supporting, providing, or delivering services for or on behalf of F4YP

Introduction

The charity has responsibility to abide by and adhere to all current UK legislation, as well as a variety of regulatory and contractual requirements.

Procedure

Physical Assets

F4YP will do the following to ensure the safeguarding of physical assets:

- Make sure investments address needs efficiently and effectively
- Regularly audit stock and quality to ensure unnecessary items are not purchased and items are replaced when needed.
- Monitor the disposal or selling of assets that are contractually bought to avoid breaches of contract.
- Follow purchase order procedures and monitor receipt of goods
- In the event of dissolution, resolve that any net assets of the charity after all its debts and liabilities have been paid, or provision has been made for them, shall on or before the dissolution of the charity be applied or transferred in any of the following ways:
    - directly for the Objects within the Articles of Association
    - by transfer to any charity or charities for purposes similar to the Objects within the Articles of Association
    - to any charity or charities for use for particular purposes that fall within the Objects within the Articles of Association

In no circumstances shall the net assets of the charity be paid to or distributed among the members of the charity (except to a member that is itself a charity) and if no resolution is passed by the members or the directors the net assets of the charity shall be applied for charitable purposes as directed by the Court or the Commission.

IT

F4YP will do the following to ensure the safeguarding of IT assets, including devices, system software, client applications and associated licences:

- Ensure assets purchased are deployed and utilised in a way deemed most effective for addressing the charity needs
- For compatibility and efficiency reasons, issue IT assets on a “fit for purpose” basis
- Ensure requests for new and replacement IT assets must go through purchase order processes and budget allocation approval
- Purchase and maintain correct licences and data protection software relevant to the charity
- Dispose of any spent equipment/devices including data cleansing correctly

Information

F4YP will do the following to ensure the safeguarding of Information assets:

- Use a secure data storage system (Microsoft 365, Salesforce)
- Password protect all devices used to access F4YP data, this can include personal devices
- Put in place confidentiality agreements for all F4YP personnel
- Put in place non-disclosure agreements and service level agreements for external providers/contractors

Breaches of policy

Any actual or suspected breach of this policy must be reported to the data protection officer via the most suitable channel, who will take appropriate action and inform the relevant internal or external authorities. Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

To be read in conjunction with:

Confidentiality policy

Data protection policy

IT and Social Media policy