



Fun 4 Young People

Information and Assets Governance Handbook



Contents

INTRODUCTION	3
DATA PROTECTION POLICY	4
IT AND SOCIAL MEDIA POLICY	7
CLIENT PRIVACY NOTICE	11
COMMUNICATIONS POLICY	14
SAFEGUARDING ASSETS POLICY	17

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	1.3.4	Communications Policy	Trustee
1.3 Information and Assets Governance	1.3.5	Safeguarding Assets Policy	Trustee

Last Edited: September 2024	Next Review: September 2026
F4YP © UNCONTROLLED IF COPIED OR PRINTED	



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 needed to be collected and processed in order 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.

The type of personal information we collect

We hold some personal information about you/your young person to make sure we can help and look after you at F4YP. For the same reasons, we get information about your young person from some other places too.

This information includes:

- Contact details
- Young person's booking/attendance records
- Young person's characteristics, such as ethnic background or any special educational needs
- Any medical conditions
- Details of any behaviour challenges

How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by you/your young person, 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 your/your young person's wellbeing and support you/your young person
- 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



We may share the information we hold with our provider organisations for them to deliver their services as part of our activity programmes. We may also share images of your young person to provider organisations and funders 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.

Providers include:

Canoe Trail
Spiral Freerun
Sophie Ibbott Therapy

Funders include:

The National Lottery Community Fund
Bedford Borough Council
Harpur Trust
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
St James Place
(last updated July 2024)

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information is:

- **Your consent.**

You may remove your consent at any time. You can do this by contacting dpo@f4yp.org

How we store your personal information

Your information is securely stored on Eventbrite and Salesforce cloud-based servers.

We keep the personal information we use 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.

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 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

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>



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 its operations or reputation, to fulfil the charity's duty of care towards the assets to which it has 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