

Data Protection Policy

This document sets out the policy for how FX Plus protects the personal data it holds, meets its legal duties as both a controller and a processor, and responds when people raise concerns about how their information is handled.

Organisation(s):	Falmouth Exeter Plus (FX Plus)
Applies to:	Everyone who processes personal data for or on behalf of FX Plus
Policy Owned by:	Executive Director
Policy Lead:	Data Protection Officer
Required Consultees:	Extended Leadership Team
Approved by:	FX Plus Board (Tier 1)
Date approved:	6 October 2026
Review date:	Three years from approval (annual review by the policy lead)
Version Number:	3.0 (draft)

Data Protection Policy

This document sets out the policy for how FX Plus protects the personal data it holds, meets its legal duties as both a controller and a processor, and responds when people raise concerns about how their information is handled.

1. Key Facts

1.1 The points below are the ones every member of staff most needs to know.

No.	Clause(s)	Description
1	6.1	Only collect and use the personal data you need, for the purpose it was collected for, and keep it accurate and secure.
2	6.3	Only access personal data you need for your job. Never use it for personal reasons.
3	8.3	Talk to the Data Protection Officer (DPO) before starting any new system, project or supplier arrangement that involves personal data.
4	13.2	Report any actual or suspected personal data breach to the DPO immediately.
5	11.2	Pass any request from a person about their own data to the DPO without delay.
6	12.3	Pass any complaint about how personal data has been handled to the Business Support Manager without delay, however it reaches you.
7	15.1	Keep personal data only as long as the Retention Schedule allows, then dispose of it securely.

2. Purpose

- 2.1 FX Plus holds personal data about many people, including staff, students, customers, visitors, and children and families who use our nursery. People trust us to look after that information, and the law requires us to do so.
- 2.2 This policy sets out FX Plus's commitment to using personal data lawfully, fairly and securely, and the principles that everyone working for us must follow. It supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025.
- 2.3 This policy says what we must do and why. How we do it is set out in the procedures and guidance listed in section 4.

3. Scope

- 3.1 This policy applies to all personal data processed by or on behalf of FX Plus, in any format. This includes paper records, electronic systems, email, and recorded images and audio.

- 3.2 It applies to everyone who handles personal data for FX Plus, including staff, agency workers, contractors and volunteers.
- 3.3 Where FX Plus processes personal data on behalf of another organisation, such as Falmouth University or the University of Exeter, we also follow that organisation's instructions and the agreement we have with it.
- 3.4 This policy does not apply to Cornwall Plus Limited, which is a separate controller with its own Data Protection Policy.

4. Related information

- 4.1 This policy is supported by the following documents, available on the staff intranet:
- Information Security Policy
 - Retention Policy and Retention Schedule (in draft)
 - Complaints Policy (in draft)
 - CCTV, Body-Worn Video and Drone policies
 - Information Breach Procedure and associated playbooks
 - Data Subject Access Request process
- 4.2 The following will be published on the FX Plus website:
- Appropriate Policy Document for special category and criminal offence data
 - Privacy notices
- 4.3 This policy also takes account of the Privacy and Electronic Communications Regulations 2003 and guidance and codes of practice issued by the Information Commission.

5. Key Definitions

- 5.1 This policy uses terms as they are defined in data protection law. The main ones are:
- **Personal data:** any information relating to an identified or identifiable living person.
 - **Special category and criminal offence data:** more sensitive personal data that the law protects more strictly, such as information about health, ethnicity, religion, trade union membership, sex life or sexual orientation, and criminal convictions or offences.
 - **Controller and processor:** the controller decides why and how personal data is used. A processor uses personal data only on a controller's instructions.
 - **Information Commission:** the UK regulator for data protection, which replaced the Information Commissioner's Office on 30 September 2026. It continues to use the ICO name.

6. Our Data Protection Principles

- 6.1 FX Plus is committed to protecting the privacy of everyone whose personal data we hold. Everyone covered by this policy must make sure that personal data is:
- used lawfully, fairly and in a transparent way;

- collected for specific and legitimate purposes, and not used in a way that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary; and
- kept secure.

6.2 FX Plus must be able to show that it complies with these principles.

6.3 Staff must only access the personal data they need to do their job and must never use it for personal reasons.

7. Our Role as Controller and Processor

7.1 FX Plus is a **controller** for personal data it uses for its own purposes. Examples include information about our staff, children and families using our nursery, customers of our services, and people recorded on our CCTV and body-worn cameras.

7.2 FX Plus is also a **processor** when it handles personal data on behalf of Falmouth University, the University of Exeter or other organisations, for example when supporting students with their wellbeing, mental health or disability. In these cases, we only process the data on the controller's documented instructions and under a written agreement.

7.3 The DPO will keep a record of the role FX Plus holds for each processing activity.

8. Accountability and Data Protection by Design

8.1 FX Plus has appointed a Data Protection Officer (DPO), who reports on data protection matters directly to the Senior Leadership Team (SLT) and has access to the FX Plus Board.

8.2 FX Plus will keep a record of its processing activities, as required by law.

8.3 Data protection must be built into new and changed systems, services, projects and supplier arrangements from the start. The DPO must be consulted at an early stage.

8.4 A data protection impact assessment (DPIA) must be completed and approved before any processing that is likely to result in a high risk to people. Examples include introducing new surveillance technology or processing sensitive data on a large scale.

8.5 All staff must complete data protection training when they join and at regular intervals after that. Staff in higher-risk roles will receive additional training.

9. Special Category and Criminal Offence Data

9.1 FX Plus will only process special category and criminal offence data where it is necessary and the law allows it. Examples include staff health records, criminal records checks through the Disclosure and Barring Service (DBS) for roles working with children and adults at risk, health information about children in our nursery, and images used to prevent and detect crime.

- 9.2 Where the law requires it, FX Plus will keep an Appropriate Policy Document that sets out the conditions we rely on and how we protect this data. We publish it on our website.
- 9.3 Extra care must be taken with personal data about children and adults at risk. Access must be limited to those who need it for their role.
- 9.4 The use of surveillance technology, including CCTV, body-worn video and drones, must follow the policies that govern it.

10. Transparency and Privacy Notices

- 10.1 FX Plus will tell people clearly how and why we use their personal data, when we collect it or as soon as possible afterwards.
- 10.2 FX Plus will publish appropriate privacy notices for the different groups of people whose personal data we process and will keep them up to date. The DPO will decide which privacy notices are needed.
- 10.3 Privacy notices will explain people's rights, including their right to complain to FX Plus and to the Information Commission.

11. Individuals' Rights

- 11.1 FX Plus will uphold people's rights under data protection law. These include the right to access their personal data, to have it corrected or erased, to restrict or object to its use, to data portability, and rights relating to automated decision-making.
- 11.2 A request can be made verbally or in writing to any member of staff. Staff must pass any request to the DPO without delay.
- 11.3 FX Plus will respond within the time limits set by law, making reasonable and proportionate searches, through the Data Subject Access Request process and related procedures.
- 11.4 FX Plus may make decisions that have a legal or similarly significant effect on a person based solely on automated processing, meaning without meaningful human involvement, only where a DPIA has been completed and the DPO has been consulted. The safeguards required by law must be in place: telling the person about the decision, letting them make representations, providing human review, and allowing them to contest it. Such decisions must not be based on special category data unless the law specifically permits it.

12. Data Protection Complaints

- 12.1 Anyone can complain to FX Plus if they believe we have not handled their personal data in line with data protection law.
- 12.2 FX Plus will:
 - make it easy to complain, including through a complaint form that can be completed online and at least one other route, such as email or post;

- accept a complaint however it is made, including through social media;
- acknowledge a complaint within 30 days of receiving it;
- look into the complaint without undue delay and keep the person informed of progress;
- tell the person the outcome, and how they can take the matter to the Information Commission if they are not satisfied; and
- keep a record of each complaint and its outcome.

- 12.3 Staff who receive a complaint about how personal data has been handled must pass it without delay to the Business Support Manager, who manages the FX Plus complaints process with advice from the DPO.
- 12.4 Where FX Plus receives a complaint about processing it carries out on behalf of another organisation, we will pass it to that organisation without delay and support it in responding.
- 12.5 The FX Plus Complaints Policy (in draft) will set out our overall approach to complaints. FX Plus will review complaint themes and use them to improve how we handle personal data.

13. Security and Personal Data Breaches

- 13.1 FX Plus will protect personal data with appropriate technical and organisational security measures, as set out in the Information Security Policy.
- 13.2 Anyone who discovers or suspects a personal data breach must report it to the DPO immediately, following the Information Breach Procedure.
- 13.3 Where a breach must be reported, FX Plus will notify the Information Commission within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk to people, FX Plus will tell them without undue delay. Where FX Plus is acting as a processor, it will notify the controller without undue delay.
- 13.4 FX Plus will record all breaches, whether they are reported or not, and act on the lessons learned.

14. Sharing Personal Data and Using Suppliers

- 14.1 Personal data must only be shared with another organisation where it is necessary and there is a lawful basis for doing so. Regular or large-scale sharing must be covered by a data sharing agreement.
- 14.2 Requests for personal data from the police or other authorities must be referred to the DPO or handled through the approved disclosure process, and every disclosure must be recorded.
- 14.3 Any supplier that will process personal data for FX Plus must be checked before it is appointed and must be bound by a written contract that includes the terms required by law.
- 14.4 Personal data must not be transferred outside the UK unless the DPO has confirmed that the transfer is lawful and appropriate safeguards are in place.

15. Retention and Disposal

- 15.1 Personal data must only be kept for as long as it is needed, in line with the Retention Policy and Retention Schedule. It must then be securely destroyed or anonymised.

16. Roles and Responsibilities

- 16.1 **FX Plus Board:** approves this policy and holds overall accountability for data protection compliance.
- 16.2 **Executive Director:** owns this policy and is accountable for its content, effect and currency.
- 16.3 **Senior Leadership Team (SLT):** makes sure FX Plus has the resources, culture and oversight needed to comply with this policy.
- 16.4 **Data Protection Officer:** leads on this policy on behalf of the Owner; advises FX Plus on its data protection obligations; monitors compliance; advises on DPIAs; and is the contact point for individuals and the Information Commission.
- 16.5 **Business Support Manager:** manages the handling of data protection complaints through the FX Plus complaints process, with advice from the DPO.
- 16.6 **Heads of service and managers:** make sure their teams follow this policy and complete training, and that processing in their area is recorded and reviewed with the DPO.
- 16.7 **All staff:** follow this policy, complete training, and report breaches, requests and complaints promptly.
- 16.8 **Suppliers and processors:** process personal data only in line with their contract and the law.

17. Compliance and Review

- 17.1 The DPO will monitor compliance with this policy and report to SLT at least once a year. Compliance may also be tested through internal audit and assurance activity.
- 17.2 Failure to follow this policy may lead to action under the relevant disciplinary procedure. Deliberately or recklessly obtaining or disclosing personal data without authority may also be a criminal offence.
- 17.3 The DPO will review this policy every year. It will be presented for re-approval at least every three years, or sooner if the law changes.

18. Equality Impact Assessment

- 18.1 The author has confirmed whether an Equality Impact Assessment is required and confirms that:

- ☒ An Equality Impact Assessment is **not required**.
- ☐ An Equality Impact Assessment **is required and has been completed**.

19. Contact for Further Information

19.1 Jonathan Hocking, Data Protection Officer. Email: dataprotection@fxplus.ac.uk.