



Policy Date: August 2026

Review Date: August 2027

Kick Start Futures

Data Protection & Confidentiality Policy

Protect • Respect • Share Appropriately • Keep Secure

Policy Date: August 2026

Review Date: August 2027

1. Policy Statement

Kick Start Futures holds personal information about students, families, staff and other people in order to provide education safely and effectively.

Some of this information is highly sensitive, including safeguarding information, SEND information, EHCPs, medical information and information about young people's personal circumstances.

Everyone working at KSF has a responsibility to protect that information.

Our approach is simple:

Only collect what we need.
Only use it for a legitimate purpose.
Only share it with people who need it.
Keep it secure.

Confidentiality is important, but it must never prevent appropriate information sharing where this is necessary to safeguard a child.

2. Purpose

This policy explains how KSF will:

- handle personal information lawfully and fairly;
- protect confidential information;
- keep records secure;
- share information appropriately;
- manage student photographs and recordings;
- respond to data breaches;
- support people's data protection rights;
- ensure staff understand their responsibilities.

3. Legal Framework

KSF will comply with applicable UK data protection legislation, including the **UK GDPR** and **Data Protection Act 2018**, together with other relevant legislation and statutory requirements.

KSF will keep its data protection arrangements under review and update them where legislation or regulatory guidance changes.

4. Data Protection Principles

Personal information will be:

- processed lawfully, fairly and transparently;
- collected for clear and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where required;
- retained only for as long as necessary;
- kept appropriately secure.

KSF will also be able to demonstrate appropriate responsibility for how personal information is handled.

5. Information KSF May Hold

KSF may need to hold information including:

- names and contact details;
- date of birth;
- emergency contacts;
- attendance;
- educational records;
- assessment and progress information;
- SEND information and EHCPs;
- medical information;
- safeguarding information;
- behaviour and incident records;
- risk assessments;
- photographs or video where appropriate;
- information supplied by commissioning schools;
- staff employment and recruitment records.

KSF will not collect information simply because it **might be useful one day**.

There should be a legitimate reason for holding it.

6. Special Category and Sensitive Information

Some personal information requires particularly careful handling.

This may include information about:

- health;
- disability;
- race or ethnicity;
- religion or belief;
- sexual orientation;
- biometric information where applicable;
- other information protected under data protection legislation.

Criminal offence information also requires appropriate safeguards.

Access to sensitive information will be limited to people who genuinely need it for their role.

7. Lawful Use of Information

KSF will identify an appropriate lawful basis when processing personal information and, where required, an additional condition for processing special category information.

Consent is **not required for every use of personal information**.

For example, information may need to be processed because of legal obligations, safeguarding responsibilities or the legitimate operation of the provision.

Where KSF does rely on consent, it will be appropriately obtained and recorded.

8. Confidentiality

Staff may become aware of highly personal information about students and families.

Staff must not:

- discuss students casually with people who do not need to know;
- discuss confidential matters in public areas of Salisbury FC;
- access records out of curiosity;
- share information through inappropriate personal accounts;
- leave confidential information where others can see it;
- disclose information to friends or family.

Confidentiality continues **outside working hours and after employment ends**.

9. Safeguarding and Information Sharing

Data protection law does **not** prevent appropriate information sharing for safeguarding purposes.

Where there is a safeguarding concern, staff should not allow fear about data protection to delay necessary action.

Staff should:

- share information with the DSL promptly;
- share only relevant information;
- use secure methods wherever possible;
- record significant safeguarding information appropriately;
- seek advice if uncertain.

Where there is an immediate safeguarding concern, **the safety of the child comes first**.

10. Working with Commissioning Schools

KSF will need to share relevant information with commissioning schools to support students' education, safeguarding and placement.

This may include:

- attendance;
- progress;
- safeguarding information;
- incidents;
- SEND information;
- risk information;
- medical information where relevant;
- placement reviews.

Information sharing will be proportionate and limited to what is reasonably required.

11. Working with Salisbury FC

KSF operates within Salisbury FC but this does **not** mean that KSF student information is automatically available to football club personnel.

Personal or confidential information about KSF students will only be shared with Salisbury FC where there is an appropriate reason.

Where information needs to be shared for safety, safeguarding or operational purposes, only the information reasonably required will be provided.

KSF records must not be left accessible within shared stadium areas.

12. Electronic Records

Electronic information must be stored using appropriate systems.

Staff will:

- use secure passwords;
- protect login information;
- lock devices when unattended;
- use approved organisational accounts;
- avoid sending confidential information to incorrect recipients;
- use secure methods when transferring sensitive information;
- report lost devices or suspected unauthorised access promptly.

Staff should take particular care when working in shared areas within Salisbury FC.

13. Email

KSF business should normally be conducted through approved KSF email accounts.

Before sending confidential information, staff should check:

- the recipient;
- whether the information needs to be sent;
- whether everyone copied into the message needs the information;
- whether attachments contain information about other students;
- whether additional security is required.

Staff should be particularly careful when using **autocomplete**, as sending student information to the wrong person can constitute a data breach.

14. Paper Records

Where paper records are required, they must be:

- stored securely;
- accessible only to authorised people;
- returned to secure storage after use;

- disposed of confidentially when no longer required.

Sensitive student information should not be left unattended in classrooms, vehicles or shared stadium areas.

15. Personal Devices

Staff should not routinely store KSF personal information on personal phones, tablets or computers.

Personal devices must not be used to photograph or film students.

Where exceptional circumstances require information to be accessed remotely, staff must follow approved KSF arrangements.

16. Photographs and Video

Photographs and video of students will only be taken and used for legitimate purposes and in accordance with appropriate consent and safeguarding arrangements.

Images must not be:

- taken using personal devices;
- posted to personal social media;
- shared informally;
- used for purposes beyond those appropriately authorised.

Particular care is required because KSF operates within a football stadium where photography and media activity may occur.

Being present at Salisbury FC does not automatically mean a KSF student can be photographed or included in club publicity.

17. Artificial Intelligence

Staff must not enter identifiable or confidential information about students, families or colleagues into publicly available AI systems unless that system has been specifically approved for such use and appropriate data protection arrangements are in place.

This includes:

- names;
- EHCP information;
- safeguarding information;
- medical information;
- reports containing identifiable details;
- incident records.

Where AI is appropriately used to support professional work, information should be anonymised where necessary and staff remain responsible for the final content.

18. Retention and Disposal

Personal information will not be retained indefinitely without reason.

KSF will maintain appropriate retention arrangements reflecting:

- legal requirements;
- safeguarding requirements;
- educational records;
- employment requirements;
- commissioning arrangements.

When information reaches the end of its appropriate retention period, it will be securely deleted or destroyed.

Safeguarding records require particular care and may need to be retained for extended periods.

19. Individual Rights

Individuals have rights in relation to their personal information under data protection legislation.

Depending upon the circumstances, these may include rights to:

- be informed about how information is used;
- access personal information;
- request correction of inaccurate information;
- request erasure in certain circumstances;
- restrict processing in certain circumstances;
- object to some types of processing.

Not every right applies in every circumstance.

Requests relating to personal information will be handled in accordance with applicable data protection requirements.

20. Subject Access Requests

A person may request access to personal information KSF holds about them.

Requests should be passed promptly to the person responsible for data protection within KSF.

Staff must not simply hand over files or email records without considering:

- the identity of the requester;
- information relating to other people;
- safeguarding information;
- legal exemptions;
- appropriate redaction.

Requests will be handled within the applicable statutory timescales.

21. Data Breaches

A personal data breach may include:

- sending information to the wrong person;
- losing paperwork;
- losing a device containing personal information;
- unauthorised access to records;
- accidentally publishing information;
- inappropriate disclosure;
- cyber incidents.

Any suspected data breach must be reported **immediately** to the Education & Provision Lead or designated data protection lead.

Staff should not attempt to hide or quietly correct a breach without reporting it.

22. Responding to a Data Breach

KSF will:

1. contain the breach where possible;
2. establish what information is involved;
3. consider who may be affected;
4. assess the potential risk;
5. record the incident;
6. take steps to reduce further harm;
7. determine whether notification is required.

Where a breach is likely to result in a risk to people's rights and freedoms, KSF will consider whether it must be reported to the **Information Commissioner's Office (ICO)** within the legally required timescale.

Affected individuals will also be informed where legally required.

23. Staff Responsibilities

All staff are responsible for protecting information they use.

Staff must:

- maintain confidentiality;
- use approved systems;
- keep records secure;
- share information appropriately;
- report breaches;
- follow safeguarding information-sharing procedures;
- ask for advice when uncertain.

A significant or deliberate breach of confidentiality may be dealt with through safeguarding or employment procedures where appropriate.

24. Data Protection Responsibility

KSF will identify who holds operational responsibility for data protection and ensure staff know who to contact for advice.

Before opening, KSF will also confirm whether its structure and processing activities require appointment of a formal **Data Protection Officer (DPO)** and ensure any applicable ICO registration/data protection fee requirements are addressed.

25. Complaints

Concerns about KSF's handling of personal information should initially be raised with KSF so that they can be investigated and resolved.

Individuals may also have the right to complain to the **Information Commissioner's Office**.

26. Training

Staff will receive appropriate information about:

- confidentiality;
- secure record keeping;
- information sharing;
- safeguarding;
- email security;
- data breaches;
- photographs and personal devices;
- AI and confidential information.

Data protection is everyone's responsibility.

27. Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Online Safety Policy;
- Staff Code of Conduct;
- SEND Policy;
- Supporting Students with Medical Conditions Policy;
- Safer Recruitment Policy;
- Complaints Policy;
- Low-Level Concerns Policy.

28. Our Commitment

KSF is trusted with information about young people's lives.

We have a responsibility to treat that information with care.

Our staff should always ask:

Do I need this information?

Do I need to share it?

Who genuinely needs to know?

Am I sharing it securely?

But when a child may be at risk, staff should never allow uncertainty about data protection to prevent appropriate safeguarding action.

Protect • Respect • Share Appropriately • Keep Secure