






Information Sharing and Data Protection Policy
Ipswich Town Football Club and Ipswich Town Community Trust

Updated Version 3- January 2021

Date of Last Review	Next Review	Who	Signature and Date
<p>Version 1- August 2019</p> <p>Version 2- November 2019</p> <p>Version 3- January 2021</p>	<p>August 2020</p> <p>November 2020</p> <p>January 2022</p>	<p>Mark Andrews</p> <p>Lauren Fellingham</p> <p>Sian Skevington</p>	<p>X  _____ Mark Andrews Safeguarding Manager</p> <p>X  _____ Lauren Fellingham Safeguarding Officer</p> <p>X  _____ Sian Skevington</p>

About us

Ipswich Town Football Club (ITFC), Ipswich Town Community Trust and Marcus Evans are the data controller in respect of all personal data collected about employees, volunteer and members of the public who visit Portman Road and the Academy. This means that we are responsible for ensuring that we do so in full compliance with data protection, GDPR and all other related privacy laws.

This Privacy Notice explains what information is collected about you, how it is used, and the steps taken to ensure that it is kept secure. We also explain your rights.

Scope

Ipswich Town Football Club and the Ipswich Town Community Trust is fully committed to protecting the rights and privacy of individuals operating in accordance with the statutory legislation outlined within the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) 2018. In doing so we are committed to protecting the privacy and confidentiality of data provided to us. Any decisions for the disclosure, retention or disposal of information are made in line with relevant legislation.

We recognise that the first priority under the Data Protection Act 1998 and General Data Protection Regulation (GDPR) 2018 is to avoid causing harm to individuals. On this basis we keep information securely in the right hands, maintain the quality of the information and retain or dispose information as appropriate.

Information about our personnel, learners and other individuals will only be used in line with established regulations. Personal data will be collected, recorded and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This may include sensitive information such as ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

Objectives

As the lawful and correct treatment of personal data is critical to our successful operations and to maintaining confidence, Ipswich Town Football Club and the Ipswich Town Community Trust is committed to operate in line with the data protection principles by:

- collecting accurate personal data only
- protecting staff, learners' and other individuals' personal details and any related records using this data fairly and only for specified lawful purposes
- handling personal data for limited, specifically stated purposes
- using personal data in an adequate and relevant manner, which is not excessive
- holding personal data only for the time period required
- maintaining personal data safely and securely
- releasing personal data only to authorised individuals/parties and not outside the UK without adequate protection and the individual's permission

- adhering to regulations and related procedures to ensure that all employees who have access to and handle any personal data held by or on behalf of Ipswich Town Football Club and the Ipswich Town Community Trust, do so in line with individual's data protection rights and are fully aware of and abide by their duties under the Data Protection Act 1998 and General Data Protection Regulation (GDPR) 2018

The Seven Golden Rules of Information Sharing. (GDPR Data Protection Act 2018)

Ipswich Town and the Ipswich Town Community Trust will ensure that they follow the golden rules of sharing information when handling personal data and information. The seven golden rules are as follows:

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

Aims of Ipswich Town and the Ipswich Town Community Trust - We will ensure that we always receive consent from individuals before using their personal data and explain fully how we will use their data and information in a written format where applicable.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

Aims of Ipswich Town and the Ipswich Town Community Trust - We will work with the Local Safeguarding Children's Board (LSCB) and the Suffolk MASH team to ensure that we seek advice when sharing information and data without consent.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

Aims of Ipswich Town and the Ipswich Town Community Trust - When there are safeguarding concerns for the immediate danger of children and vulnerable adults, Ipswich Town will pass on the relevant data to police, social services and other agencies with our local council to ensure the safety and wellbeing of the individual. We will ensure that we only pass on the relevant information and if there is no consent, we will endeavour to ensure we consider the opinion and the requests of the individual.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

Aims of Ipswich Town and the Ipswich Town Community Trust - We will always consider the safety and well-being of the individual and the impact our actions may have on other individuals around the concerned. We will ensure that we liaise with local safeguarding teams to ensure the correct decisions are made.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up to-date, is shared in a timely fashion, and is shared securely (see principles).

Aims of Ipswich Town and the Ipswich Town Community Trust - We will ensure that when information or data is shared it is shared only with those that it is necessary for and ensure that all records are kept up to date when sharing information and shared securely. When sharing data this is done via a password protected file sharing programme which only the recipient will have access to.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Aims of Ipswich Town and the Ipswich Town Community Trust - We will ensure that we always keep timely records of all information sharing and data specifically that surrounding safeguarding concerns.

Information sharing- Advice for practitioners providing safeguarding services to children, young people, parents and carers (July 2018)

When and how we will share information

Ipswich Town and the Ipswich Town Community Trust will consider the following questions when deciding if and when to share information. This will inform us further about how we share this information and the severity of the need:

Is there a clear and legitimate purpose for sharing information?

- Yes – see next question
- No – do not share

Do you have consent to share?

- Yes – you can share but should consider how.
- No – see next question

Does the information enable an individual to be identified?

- Yes – see next question
- No – you can share but should consider how.

Have you identified a lawful reason to share information without consent?

- Yes – you can share but should consider how.
- No – do not share

How

- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right individual
- Ensure where possible that you are sharing the information securely
- Where possible, be transparent with the individual, informing them that that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual. All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage you are unsure about how or when to share information, you should seek advice on this. You should also ensure that the outcome of the discussion is recorded.

If dealing with the safety and well-being of a child that is in immediate risk, ensure that all relevant information is passed on to the relevant authorities as quickly as possible.

Guidance taken from *Information sharing- Advice for practitioners providing safeguarding services to children, young people, parents and carers (July 2018)*

How we process and handle data

Anyone processing personal data at Ipswich Town and the Ipswich Town Community Trust will comply with the enforceable principles of data protection. Personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for only specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purpose(s) for which it is processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of individuals for no longer than is necessary for the purpose(s) for which it is processed;
- processed in a manner that ensures its security by appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

Fair and lawful processing

This Policy aims to ensure that our data processing is done fairly and without adversely affecting the rights of the individual. Lawful processing means data must be processed on one of the legal bases

set out in the GDPR. When special category personal data is being processed, additional conditions must be met.

Processing for limited purposes

Ipswich Town and the Ipswich Town Community Trust collect and processes personal data. This is data we receive directly from an individual and data we may receive from other sources. We will only process personal data for the purposes of the Ipswich Town and the Ipswich Town Community Trust] or EFL, or as specifically permitted by the GDPR. We will let individuals know what those purposes are when we first collect the data or as soon as possible thereafter.

Consent

One of the lawful bases on which we may be processing data is the individual's consent. An individual consent to us processing their personal data if they clearly indicate specific and informed agreement, either by a statement or positive action. Individuals must be easily able to withdraw their consent at any time and withdrawal must be promptly honoured. Consents should be refreshed every season. Explicit consent is usually required for automated decision-making and for cross-border data transfers, and for processing special category personal data. Where children are involved then the consent must be in written from parent/guardian

Where consent is our legal basis for processing, we will need to keep records of when and how this consent was captured.

Notifying individuals

Where we collect personal data directly from individuals, we will inform them about:

- the purpose(s) for which we intend to process that personal data;
- the legal basis on which we are processing that personal data;
- where that legal basis is a legitimate interest, what that legitimate interest is;
- where that legal basis is statutory or contractual, any possible consequences of failing to provide that personal data;
- the types of third parties, if any, with which we will share that personal data, including any international data transfers;
- their rights as data subjects, and how they can limit our use of their personal data;
- the period for which data will be stored and how that period is determined;
- any automated decision-making processing of that data and whether the data may be used for any further processing, and what that further processing is.
- If we receive personal data about an individual from other sources, we will provide the above information as soon as possible and let them know the source we received their personal data from;
- We will also inform those whose personal data we process that we, the [Club], are the data controller in regard to that data, and which individual(s) in the [Club] are responsible for data protection.

Adequate, relevant and non-excessive processing

- We will only collect personal data that is required for the specific purpose notified to the individual.

- You may only process personal data if required to do so in your official capacity with Ipswich Town and the Ipswich Town Community Trust. You cannot process personal data for any reason unrelated to your duties.
- Ipswich Town and the Ipswich Town Community Trust must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised.

Accurate data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at the start of each season. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely processing

We will not keep personal data longer than is necessary for the purpose(s) for which they were collected. We will take all reasonable steps to destroy or delete data which is no longer required, as per our Privacy Notice.

Processing in line with data subjects' rights

As data subjects, all individuals have the right to:

- be informed of what personal data is being processed;
- request access to any data held about them by a data controller;
- object to processing of their data for direct-marketing purposes (including profiling);
- ask to have inaccurate or incomplete data rectified;
- be forgotten (deletion or removal of personal data);
- restrict processing;
- data portability;
- and not be subject to a decision which is based on automated processing.

Ipswich Town and the Ipswich Town Community Trust is aware that not all individuals' rights are absolute, and any requests regarding the above should be immediately reported to the Club.

Data security

- We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
- We have proportionate procedures and technology to maintain the security of all personal data.
- Personal data will only be transferred to another party to process on our behalf (a **data processor**) where we have a GDPR-compliant written contract in place with that data processor.
- We will maintain data security by protecting the confidentiality, integrity and availability of the personal data.
- Our security procedures include:
 - **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
 - **Secure desks, cabinets and cupboards.** Desks and cupboards should be locked if they hold personal data.

- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed.
- Screens and monitors must not show personal data to passers-by, and should be locked when unattended. Excel spreadsheets will be password protected.
- **Personal Devices.** Anyone accessing or processing Ipswich Town and the Ipswich Town Community Trust's personal data on their own device, must have and operate a password only access or similar lock function, and should have appropriate anti-virus protection. These devices must have Ipswich Town and the Ipswich Town Community Trust's personal data removed prior to being replaced by a new device or prior to such individual ceasing to work with or support Ipswich Town and the Ipswich Town Community Trust.

Employees and Volunteers at Ipswich Town

The information we collect and its sources

When you apply for a position at Ipswich Town and the Ipswich Town Community Trust we will obtain some personal data from you to enable us to make recruitment decisions.

Typically we will record:

- name
- date of birth
- contact details
- qualifications and experience
- information about your right to work in the UK
- ethnicity and other equality and inclusion information
- information about your criminal record (if applicable)

If you are successful and accept an offer of work with us, we will obtain additional information which will form part of your personnel records. This may come from you or your previous employer(s).

This will normally include:

- details of your bank account and national insurance number
- medical information (allergy / disability information and medical needs)
- doctor and contact details
- next of kin and emergency contact details
- details of periods of leave taken by you, including holiday, sickness absence, family leave, and the reasons for the leave

During the course of your employment we will add:

- appraisal records
- training details
- details of any disciplinary or grievance procedures in which you have been involved

We will also add supplementary information such as any medical or occupational health reports.

How we will use your information

We will primarily use the personal information:

- **Selection.** For making recruitment and promotion decisions
- **Communication.** To communicate with you or your nominated representative
- **Records keeping.** For record keeping purposes, such as keeping details of any equipment we provide to you such as laptop computers
- **Administration.** For internal administration, including payment of remuneration and expenses, obtaining insurance, making travel and accommodation arrangements
- **Security.** To ensure security of our premises and assets
- **Health and welfare.** Addressing any medical or other specific needs you may have
- **Equal opportunities.** To enable us to monitor and ensure compliance with anti-discrimination policies or to comply with our legal obligations relating to social inclusion
- **Compliance.** Ensuring compliance with your contract of employment and our legal obligations
- **Appraisals and training.** Monitoring your suitability for your role or any other role and assessing your needs for and provision of training and support
- **Disciplinary matters**
- **Health and safety.** To ensure a safe environment for you and your colleagues

Consent and lawful processing of personal data

The legal basis for the collection and processing of your personal data is:

- **For selection.** that it is necessary to fulfil the contract that you wish to enter into with us and it is necessary to carry out obligations in the field of employment or relates to personal data that is manifestly made public by you
- **for dealing with medical needs:** that you have given your explicit consent or, in serious cases that it is in your vital interests to help you
- **for equality and inclusion and health and safety:** that it is necessary for us to comply with our legal obligations
- **Safeguarding:** that it is necessary for the purposes of protecting the employee or volunteer from neglect or physical, mental or emotional harm
- **in all other cases:** that it is necessary for the performance of the contract of employment that you have entered into or are taking steps to enter into

Disclosing your personal information

We will limit who, within ITFC, has access to your personal data such that it will be accessible on a need to know basis. This will include members of the Human Resources department and your line manager with relevant information being provided to the Finance department so that they can pay your expenses (where appropriate).

We may disclose relevant personal data to third parties:

- **DBS.** Where your role requires you to have a Disclosure and Barring Service (DBS) check, we will provide details to the relevant agency in order to obtain a DBS certificate for you.
- **HMRC.** We will provide relevant personal data to HM Revenue & Customs for tax and payroll purposes.
- **Insurers**
- **Medical / occupational health practitioners.** We may provide relevant details to enable you to receive treatment or support.
- **Disciplinary panels / your representative(s).** If you are involved in a disciplinary matter or other legal or similar process.
- **Law enforcement,** the Independent Safeguarding Authority, relevant local authorities (including the Local Authority Designated Officer (also known as 'LADO')) and/ or the police
- **Legal or other professional advisers** including panel members who deal with issues relating to DBS checks
- **Reference requests.** If you require us to provide a reference for you, we will disclose relevant personal data.

Data retention

We will normally keep your principal records for as long as you are a member of staff with Ipswich Town and the Ipswich Town Community Trust and for 7 years afterwards.

After this time, we will keep historical records of your achievements and any incidents at Ipswich Town and the Ipswich Town Community Trust and will anonymise the other information and keep it for analysis of roles and trends.

Updating and correcting your information

We encourage you to inform your line manager or Denise Booth in the Human Resources department of any updates to your personal information as soon as possible.

If you are providing updates or corrections about another person, we may require you to provide us with proof that you are authorised to provide that information to us.

Your rights

Where you have given your consent to any processing of personal data, you have the right to withdraw that consent at any time. If you do, it will not affect the lawfulness of any processing for which we had consent prior to your withdrawing it.

You have the right of access to your personal data and, in some cases, to require us to restrict, erase or rectify it or to object to our processing it, and the right of data portability.

If you want to exercise any of your rights, you should contact Denise Booth in the Human Resources department.

Allegations Reporting Procedure

Reporting a personal data breach:

- In the case of a breach of personal data, we may need to notify the applicable regulatory body and the individual.
- If you know or suspect that a personal data breach has occurred, inform Denise Booth in the HR department immediately, who may need to escalate as appropriate. You should preserve all evidence relating to a potential personal data breach.