Harrogate Town AFC Privacy Policy

1.0 Responsibilities

Name of company Harrogate Town AFC Limited ("HTAFC"). Company number 02523873. Registered office: Quay Point, lakeside, Doncaster DN4 5PL

Responsible person The Data Protection Officer will act as the first contact for all data protection correspondence. Where specialist assistance is needed, this will be sourced from Strata Homes Limited and specialist external organisation for more complex privacy queries.

2.0 About this Policy

This Policy is to help the HTAFC with data protection matters internally. This should be made available to all staff members, volunteers and others who come into contact with personal data during the course of their involvement with HTAFC.
We will follow and reference a number of legislations regarding data including: The Privacy and Electronic Communications Regulations (PECR), The Data Protection Act (DPA) 2018 and General Data Protection Regulation (GDPR).

HTAFC 2 x notices and 1 x policy relating to data;
- Harrogate Town AFC Privacy Notice
- Harrogate Town AFC Privacy Policy
- Cookies Notice

2.1 Leglistation

HTAFC understand the current legislation and throughout this policy we establish ways in which we adhere to it. The relevant legislation is listed below.

2.1.1 The Privacy and Electronic Communications Regulations (PECR)

Giving people specific privacy rights in relation to electronic communications.
With specific rules on:
- Marketing calls, emails, texts and faxes; cookies (and similar technologies);
- Keeping communications services secure;
- And customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

2.1.2 Data Protection Act (DPA) 2018

This Act applies in different situations and performs different functions. It sets out four separate data protection regimes:

Part 2 Chapter 2: Supplements and tailors the GDPR- This covers elements covered in the GDPR but adds to and tailors them.

Part 2 Chapter 3: Extends a modified GDPR- This extends the GDPR to some other (rare) cases, e.g. the principles for processing data are extended if you are a public authority to unfiled papers and notes to ensure that freedom of information rules work properly.

Part 3: Law enforcement authorities- This sets out a separate data protection regime for authorities that are processing personal data for law enforcement purposes, e.g. you can process criminal convictions data if processing satisfies the substantial public interest test.

Part 4: Intelligence services- This sets out a separate data protection regime for the intelligence services - MI5, MI6, and GCHQ – and their processors, e.g. personal data should not be transferred to a country outside the UK or to an international organisation unless the transfer is necessary for the purposes of that controller's statutory function, or for purposes provided for in the Security Services Act 1989 or the Intelligence Services Act 1994.

2.1.3 Data protection principles of GDPR

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals; b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
b. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
c. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
d. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
e. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2.2 General provisions

a. This policy applies to all personal data processed by HTAFC.
b. The Responsible Person shall take responsibility for HTAFC's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. HTAFC shall register with the Information Commissioner's Office as an organisation that processes personal data.

2.3 Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, HTAFC shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

2.4 Lawful purposes

a. All data processed by HTAFC must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. HTAFC shall note the appropriate lawful basis in the Register of Systems. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in HTAFC's systems.

2.5 Data minimisation

a. HTAFC shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

2.6 Accuracy

a. HTAFC shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

2.7 Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, HTAFC shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why. The Data Protection Officer will communicate processes with staff, that include the routine and regular checking of data to ensure that we still need to store it.

2.8 Security

a. HTAFC shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

2.9 Data breach policy

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.
Any one who works with data at HTAFC will be provided with a copy of this policy and will be required to notify the 'Data Controller' i.e. the data Protection Officer, of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under HTAFC's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment and is not intended to have contractual effect.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

3.0 Definitions

Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special category data
Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Personal data breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Data subject
The person to whom the personal data relates.

ICO
ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

4.0 Responsibility

The Data Protection Officer (DPO) at HTAFC has the immediate responsibility for breach notification within HTAFC. The DPO is responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

The Board of Directors have an obligation to be aware of and enforce legal compliance. The policy will also be annually reviewed at Board level, with updates provided through reporting via the DPO.

The DPO is responsible for overseeing this policy and developing privacy related notices and guidelines. If you have any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed you should contact the DPO at dataprotection@harrogatetownafc.com.

5.0 Security and data-related policies

Staff and volunteers should refer to the following policies that are related to this data protection policy:
- Privacy Notice which sets out what data is being collected by HTAFC, what happens to the data and the subject's rights.
- Cookies Notice which refers to the use of data upon accessing the HTAFC's website.

6.0 Data breach procedure

6.1 What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed. Examples of a data breach could include (but are not limited to) the following:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

6.2 When does a breach need to be reported?

HTAFC must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others. If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

6.3 Reporting a data breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

a) Complete a ICO data breach report form (which can be obtained from the ICO website (www.ico.org.uk)
b) Email the completed form to the DPO
c) Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout HTAFC and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from the DPO.
d) Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The DPO will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the Board of Directors' representative.

6.4 Managing and recording the breach

On being notified of a suspected personal data breach the DPO (in consultation with the Board of Directors) will take immediate steps to establish whether a personal data breach has in fact occurred. If a breach is deemed to have occurred the following steps should be taken:

a) Where possible, contain the data breach;
b) As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
c) Assess and record the breach in HTAFC's data breach register;
d) Notify the ICO;
e) Notify data subjects affected by the breach;
f) Notify other appropriate parties to the breach;
g) Take steps to prevent future breaches.

6.5 Notifying the ICO

The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals. This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If HTAFC is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

6.6 Notifying data subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO will notify the affected individuals without undue delay. The DPO will inform the data subject of the likely consequences of the data breach and the measures HTAFC have (or intend) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach the DPO will co-operate with and seek guidance from the Board of Directors, Strata Homes Limited (as the parent company), relevant external agencies, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then HTAFC will consider alternative means to make those affected aware (for example by making a statement on the HTAFC website).

6.7 Notifying other authorities

HTAFC will need to consider whether other parties need to be notified of the breach. For example:

- Insurers;
- programme participants;
- third parties (for example when they are also affected by the breach);
- local authority;
- the police (for example if the breach involved theft of equipment or data).

6.8 Assessing the breach

Once initial reporting procedures have been carried out, HTAFC will carry out all necessary investigations into the breach. HTAFC will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data). Having dealt with containing the breach, HTAFC will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- what type of data is involved and how sensitive it is;
- the volume of data affected;
- who is affected by the breach (i.e. the categories and number of people involved);
- the likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- what has happened to the data;
- what could the data tell a third party about the data subject;
- what are the likely consequences of the personal data breach on HTAFC; and,
- any other wider consequences which may be applicable.

6.9 Preventing future breaches

Once the data breach has been dealt with, HTAFC will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- establish what security measures were in place when the breach occurred;
- assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- consider whether its necessary to conduct a data protection impact assessment;
- consider whether further audits or data protection steps need to be taken;
- update the data breach register;
- debrief the Board of Directors following the investigation.

7.0 Disclosure of your information

We do not share your information with any other third party without your agreement unless we are under a duty to disclose or share your personal data in order to comply with any legal or tax obligation, or in order to enforce or apply our terms the employment contract; or to protect the rights, property, or safety of HTAFC or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection.

We will share your information with future employers on your request.

Any third party providers used by us to fulfil our contractual obligations to you will only collect, use, store and disclose your information in the manner and to the extent necessary for them to provide their services to us. We have written agreements in place with each third party to ensure that your information is kept securely, is not used for any other purpose and is deleted when no longer required.

Such third party providers may include:
• Sage Payroll
• Howard Matthews Accountancy/Elite Payroll
• Pension company
• Private healthcare
• Life assurance and insurance companies
• Strata Homes (IT)
• Travel and accommodation booking services
• Training providers
• Funding providers
• HMRC
• Department of Work & Pensions
• HSE
• Police

We may share personal information with other organisations such as the Premier League, the English Football League, the Office for National Statistics and other governing bodies compliance purposes, research, reporting and improvement of strategic planning and business decisions or funding. We never sell personal information to third parties.

7.1 Who HTAFC will share information with

Part of the decision-making process will include consideration about who to share information with. This could include:

- Statutory organisations - the police and/or children's services must be informed about child protection concerns. Local authority designated officers/teams must be consulted where there are concerns about someone in a position of trust. In order to protect or maintain the welfare of our participants, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies. If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- Disclosure & Barring Service - must be informed of any concerns about someone in regulated activity who is suspended or expelled from the organisation.
- Other clubs and other sports organisations - informing other organisations needs to be considered according to the principles above in order that they can safeguard children in their care who may be at risk of harm.
- Individuals within the organisation - this will include members of the safeguarding team (see the charities safeguarding policies for names and contact details of our designated officers) and key staff members on a strictly 'need to know' basis in order to keep children and vulnerable adults safe according to the principles above.
- HTAFC safeguarding records contain sensitive personal information and are treated as highly confidential. They will not be disclosed except where information sharing is in the interests of protecting a child from significant harm or potential harm as the welfare and protection of children and young people is always the paramount consideration (Children Act 1989).

8.0 Access to data and disclosure staff

We are legally obliged to protect certain information on our staff. HTAFC staff have a right to see records of their personal information. Staff who wish to access this information can make a subject access request under the Data Protection Act 1998.

Disclosure of these records will be made once third party information has been removed in accordance with the Data Protection Act 1998. HTAFC staff will have restricted access to

participants' personal data and will be given access only on a 'need to know' basis in the course of their duties within the charity.

Third parties personal data about participants will not be disclosed to third parties without the consent of the participant or the child's parent or carer, unless it is obliged by law or in the best interest of the child.

9.0 Data sharing agreements

If there is a need to share additional information on a one-off-basis, the parties concerned should consider whether the sharing is necessary to the agreement and document their considerations/findings, including any consent sought (and if not sought, an explanation as to why).

If additional information is required on a repeated basis over and above what is defined in this agreement, to enable the agreement to achieve its aims, the lead officers for each organisation should agree an addition to the sharing agreement, ensuring that the new information meets the same legislative basis as the original. This addition should be added to the agreement and all parties should sign up to it.

Our data sharing table outlines some of the data that might be shared and why. We have also set out a template data sharing agreement that will be used when any arrangements for data sharing will be put into place.

10.0 Training

If staff do not receive appropriate training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the GDPR and other national data protection legislation resulting in regulatory action and/or reputational damage to the organisation. Therefore training in data protection and data privacy will be delivered to everyone at HTAFC. Training will include:

- a needs based training programme, developed for all staff and specific to HTAFC;
- Board of Directors training, on the basis that they are responsible for legal compliance;
- a training programme that incorporates regional and national sector specific requirements in key areas such as;
    - Data Protection / GDPR
    - information security
    - records management
    - data sharing
    - requests for personal data

Training will mainly be delivered virtually through workshops whenever legislation means a change in process or procedures, however regular staff training might take place in person.

Training needs will be assessed regularly for full time, part-time, casual staff and volunteers who come in to contact with data. Training undertaken will be recorded and renewal dates planned and communicated.

Induction training. Each new member of staff (including volunteers) will undertake training (normally within 1 month of joining HTAFC) before they access any data. Training will focus on the key areas outlined previously in this policy.

Training materials will be available to any member of staff/volunteer who would like to refresh their understanding. Refresher training will be provided as required, or whenever there are significant legislation changes. Some staff may need specialist training, which can be arranged as required.

Quality checks: The DPO will carry out regular spot checks to ensure compliance with this policy. As well as tests that check staff understanding of the policy. All training will be recorded and made available for authorities to view on request.

11.0 Reporting data protection concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the DPO or your line manager. This can help capture risks as they emerge, protect HTAFC data breaches and keep our processes up to date and effective.

12.0 Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and updates as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to HTAFC.