



BYCC
Your Community Centre

Bridport Youth and Community Centre BYCC GDPR Data Protection Policy

PRINCIPLES OF GDPR The General Data Protection Regulations (GDPR) are in force from 25th May 2018. GDPR provides increased protection for EU citizens regarding their personal data by placing responsibilities on organisation who gather and utilise this data in the course of their operations.

GDPR is based on a set of 7 principles that must be adhered to:

- **Fair, lawful and transparent processing:**
Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **The purpose limitation principle:**
Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
- **Data minimisation:**
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- **Accuracy:**
Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay
- **Data retention periods:**
Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security:**
Personal data must be processed in a manner that ensures appropriate security of that data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability:**
The controller is responsible for, and must be able to demonstrate, compliance with the Data Protection Principles.

Definitions: In this policy, the following words and phrases have the following meanings:

- **BYCC:** means the Bridport Youth and Community Centre Trust.
- **Consent:** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.
- **Criminal Records Personal Data:** means personal data relating to criminal convictions and offences and personal data relating to criminal allegations and proceedings.
- **Data Protection Legislation:** means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any other applicable primary or secondary legislation as may be in force in the UK from time to time.
- **Data Subject:** means a living identified or identifiable individual about whom BYCC holds personal data.
- **Member of Staff:** is any trustee, employee, worker, volunteer, contractor and consultant employed or engaged by BYCC.
- **Users:** means any person who hires or uses the facilities of the BYCC
- **Members:** any young person is a member or attends the youth club activities of BYCC
- **Personal Data:** is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data i.e. where all identifying particulars have been removed.
- **Processing:** is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.
- **Special Categories of Personal Data:** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject's sex life or sexual orientation.

Introduction: This policy sets out how BYCC processes the personal data of data subjects, including the personal data of job applicants and the personal data of its current and former trustees, employees, workers, volunteers, contractors, consultants, clients, users, members, customers, suppliers and other third parties. It applies to all personal data that BYCC process, regardless of the media on which those personal data are stored e.g. electronically, on paper or on other materials. BYCC is committed to being clear and transparent about how it collects and uses personal data and to complying with its data protection obligations.

Protecting the confidentiality, security and integrity of the personal data that BYCC process is also of paramount importance to its business operations.

BYCC will process all personal data in accordance with this policy, the data protection legislation and the latest privacy notice which has been issued to you.

This policy applies to all members of staff. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.

A member of staff / volunteer / user; are also data subjects and may also process personal data on the Trust's behalf about other data subjects. This policy should therefore be read and interpreted accordingly. By all persons processing data. They must always comply with it when processing personal data on the Trust's behalf in the proper performance of their job duties and responsibilities. The data protection legislation contains important principles affecting personal data relating to data subjects. The purpose of this policy is to set out what the Trust expects from staff and volunteers to ensure they understand and comply with the rules governing the processing of personal data to which they have access in the course of your work - so as to ensure that neither the Trust nor staff and volunteers breach the data protection legislation.

BYCC takes compliance with this policy very seriously. Any breach of this policy - or any breach of the data protection legislation - will be regarded as misconduct and will be dealt with under the Trust's disciplinary procedure. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (or procuring their disclosure to a third party) without the Trust's consent, constitutes a gross misconduct offence and could lead to your summary dismissal. If you are not an employee or volunteer, you may have your contract with BYCC terminated with immediate effect.

BYCC's **Data Compliance Manager** has responsibility for data protection compliance within the Centre. They should be contacted for any questions about the operation of this policy or if further information is needed about the data protection legislation, or there any concerns that this policy is not being or has not been followed.

They can be contacted as follows:

Data Compliance Manager	
Name	Katrina Polanska
Job Title	Centre Manager
Telephone Contact	01308 422009
Email	bridportycc@gmail.com
Postal Address	Bridport Youth & Community Centre, Gundry Lane, Bridport DT6 3RL

You must also contact them to seek further advice in the following circumstances:

- If you are in any doubt about what you can or cannot disclose and to whom
- If you are unsure about the lawful basis you are relying on to process personal data
- If you need to rely on consent to process personal data
- If you need to obtain or issue privacy notices
- If you are not clear about the retention period for the personal data being processed
- If you are unsure about what appropriate security measures you need to implement to protect personal data
- If you need assistance in dealing with any rights invoked by a data subject
- If you suspect there has been a personal data breach
- Where you propose to use personal data for purposes other than that for which they were collected
- Where you intend to engage in a significant new or amended data processing activity
- Where you plan to undertake any activities involving automated decision-making, including profiling
- If you need assistance with, or approval of, contracts in relation to sharing personal data with third-party service providers
- If you believe personal data are not being kept or deleted securely or are being accessed without the proper authorisation
- If you suspect there has been any other breach of this policy or any breach of the data protection principles.
- If you wish to make an internal complaint that this policy is not being - or has not been - followed, you can also raise this as a formal grievance under the Trust's grievance procedure.

The Data Protection Principles: Under the data protection legislation, BYCC and all members of staff must comply with at all times in their personal data processing activities.

BYCC is responsible for, and must be able to demonstrate compliance with, these data protection principles. This is called the Principle of Accountability.

Lawfulness, fairness and transparency: Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle means that both BYCC and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

Lawfulness and fairness: The data protection legislation provides that processing is only lawful in certain circumstances. **These include where:**

- The data subject or a responsible person / parent / carer has given consent to the processing of personal data for one or more specific purposes
- The processing is necessary for the performance of a contract with the data subject, for the purpose of record keeping for members and users
- The processing is necessary for compliance with BYCC's legal obligations
- The processing is necessary to protect the data subject's vital interests (or someone else's vital interests)
- The processing is necessary to pursue BYCC's legitimate interests (or those of a third party), where the data subject's interests or fundamental rights and freedoms do not override BYCC's interests; the purposes for which BYCC process personal data for legitimate interests must also be set out in an appropriate privacy notice.

BYCC and members of staff must only process personal data on the basis of one or more of these lawful bases for processing. Before a processing activity starts for the first time, and then regularly while it continues, BYCC will review the purpose of the processing activity, select the most appropriate lawful basis (or bases) for that processing and be satisfied that the processing is necessary for the purpose of that lawful basis (or bases). When determining whether the Trust's legitimate interests are the most appropriate basis for lawful processing, BYCC will conduct a legitimate interest's assessment, keep a record of it and keep it under review.

Where BYCC relies on consent as the lawful basis for processing, this requires the data subject to have given a positive statement, active opt-in or clear affirmative action.

The BYCC collects data for current and former trustees, employees, workers, volunteers, contractors, consultants, clients, users, members, customers, suppliers and other third parties, with the following details and reasons:

What is personal data:

Personal data is any data about, or that identifies you, the individual.

Personal data can vary in its nature and consists of:

Contact data: e.g., name, contact details (email, phone, address etc.)

Personal data: e.g. date of birth, gender, ethnicity etc.

Financial: e.g. account details, credit/debit card details, financial transactions

What personal data do we collect:

When you join the BYCC youth clubs we may collect information about you. This may include any of the examples above, why you are interested in BYCC youth clubs, interactions you have had with us and other information relating to you personally which you may choose to provide to us.

Data protection law recognises that certain types of personal information are more sensitive. This is known as 'sensitive' or 'special category' personal information and covers information revealing racial or ethnic origin, religious or philosophical beliefs and political opinions, trade union membership, genetic or biometric data, information concerning health or data concerning a person's sex life or sexual orientation.

Sensitive information will only be collected where necessary, for example, we may need to collect health information from you when you register for an activity. We may need to understand more about your background to support the monitoring of the effectiveness of our activities and or social media. Clear notices will be provided at the time we collect this information, stating what information is needed, and why and which parts are optional.

With your explicit consent, we may also collect sensitive personal information if you choose to tell us about your experiences in BYCC for use in research or a case study.

BYCC will only collect personal data to the extent that they are required for the specific purposes notified to the data subject and will not process personal data for any reason which is unrelated to your job duties and responsibilities. In addition, you must ensure that any personal data you collect are adequate and relevant for the intended purposes and are not excessive. This includes special categories of personal data and criminal records personal data.

Why we collect personal data and how we use it:

BYCC offers a wide range of opportunities to young people through our activities. In addition to these activities we work with young people outside the youth clubs and youth workers to influence policy makers by ensuring that young people are given a voice and appropriate channels to be heard. We also provide support to individuals and organisations that support young people.

We collect data in order to administer, deliver and monitor our services and support to young people and youth organisations, to fundraise and generate funds to support our work, to support our campaigns, respond to enquiries, and to meet our contractual and legal obligations.

BYCC have strict safety and safeguarding policies in place which means that in addition to collecting data about our employees and volunteers for the purpose of their role with us, we capture other data in relation to criminal records.

In order to make what we do happen and to improve the lives of young people, we use personal data in the following ways:

- To administer the membership of youth organisations and provide and promote a range of support, opportunities and benefits to youth organisations
- To administer and monitor young people's participation on our activities and the impact and outcomes for young people
- To undertake research and analysis to develop and promote policy and practice
- Promote opportunities to young people
- To involve people in policy and advocacy work including research, events and responding to media opportunities
- To promote the BYCC (using media content) through websites, social media, promotional materials, publications, press releases or other illustrations of our work
- To engage current and potential funders and fundraisers with opportunities to support our work and make what we do possible
- To process financial payments, donations and claim Gift Aid
- To ensure that all those working for BYCC have had relevant checks to work with children, young people and vulnerable adults
- To employ and manage staff and volunteers and manage applications.
- To respond to enquiries and complaints
- To undertake due diligence to manage risks

How we collect personal data:

Direct from the individual

BYCC collect data directly from individuals (e.g., young people, youth workers, teaching staff, fundraisers, funders, donors, current and potential employees, trustees etc.) and those with parental/guardian responsibility for a young person.

When information is collected, we will explain what it is for and be clear about elements that are optional.

Third parties and external sources

Where data is collected from an external source (i.e. not directly from the individual) and is to be held or use beyond the specific activity or event, we will notify the individual that we have obtained their data, how we intend to use it, and if required, capture consent to market membership, funding opportunities and our services in the future.

Using media content (photo, video and audio content)

To help promote the value of our work BYCC take a range of photographic, video and audio content. Photos, videos and audio content may be used by BYCC, or by our event partner(s) (including funders) and member organisations on websites, social media, promotional materials, publications, press releases or other illustrations of our work.

We will ask for consent from individuals that will be used in photos where they may be identifiable. Where the individual is under the age of 18 or a vulnerable adult we will seek consent of the parent/guardian. Consent can be withdrawn at any time (see 'Withdrawing your consent' section). If consent is withdrawn we will stop using the photos/videos/audio content for future purposes but may not be able to retract publications already in the public domain.

How you can withdraw your consent:

BYCC capture consent for a number of its activities (identified above 'How we use personal data').

Consent can be withdrawn at any point by:

Unsubscribing from an email or newsletter

By contacting the **Data Compliance Manager / Safeguarding Lead / Trust Chairperson**

Young people and members participating in activities can withdraw their consent at any point by contacting us; however this may impact their ability to fully participate in the activity.

How we store and secure data:

Securing personal data

BYCC take its responsibility to protect personal data seriously. We ensure that our data is held securely within our main database and on our network. We use a range of tools and technologies to capture, process and store data securely. Only authorised employees and partners (employability programme), and those who process data on our behalf (e.g. software suppliers) have access to data. BYCC have a strict Data Protection Policy and data sharing agreements in place to ensure that appropriate processes, procedures and best practice is in place to protect personal data. Only the data that is necessary to perform the task is accessed and processed.

How we share personal data

BYCC does not sell any personal data that we hold. BYCC shares personal data with the following parties:

Member organisations and partners delivering our activities (for the purposes of safety and access to opportunities)

Funders will receive aggregated and anonymised statistics only. These are shared with funders to demonstrate the impact of participation in our activities.

HMRC and other organisations for the performance of employee contracts and processing Gift Aid payments

Social Services, emergency services, the Health and Safety executive, local authorities and the police in the event of an emergency or in the event of a safeguarding issue (e.g. there is a risk to the safety of a young person or any other party) or to law enforcement agencies for the prevention and detection of crime

Where we have a legal or regulatory obligation we will share data/information with the police, law enforcement agencies, the Government and statutory agencies or any other necessary parties

The Disclosure and Barring Service (DBS) for the purposes of verifying suitability of those working with children and young people

Third party suppliers:

We may need to share your information with data hosting providers or service providers who help us to deliver our services, projects, or fundraising activities and appeals. These providers will only act under our instruction and are subject to pre-contract scrutiny and contractual obligations containing strict data protection clauses. We also may need to share your names with partners and venues hosting events for the purpose of registration.

How long do we keep personal data?

BYCC will only store your data for as long as necessary and in line with the original purpose(s) that it was collected. BYCC collect, store and process personal data in line with our Data Protection Policy and have strict retention schedules outlined and adhered to in our Data Retention Policy.

BYCC also comply with its legal obligations to keep certain data for a period of time (e.g. Gift Aid declarations and financial transactions).

BYCC will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes special categories of personal data and criminal records personal data.

When personal data are no longer needed for specified purposes, you must ensure that they are destroyed, erased or anonymised in accordance with BYCC's rules on data retention and destruction set out below.

Storage limitation: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

Retention of data relating to youth club members:

BYCC will generally hold personal data, until 6 months of non-attendance.

Overall, this means that BYCC will thin the file of personal data that is held members for members 6 months after their last visit. BYCC only continue to retain for a longer period what is strictly necessary and for anonymised statistics only.

Retention of data relating to job applicants: If a job applicant's application for employment or engagement is unsuccessful, BYCC will generally hold their personal data, including special categories of personal data and criminal records personal data, for **six months** after the end of the relevant recruitment exercise but this is subject to:

Any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records

The retention of some types of personal data for up to six years to protect against legal risk e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court.

If the job applicant has consented to BYCC keeping their personal data on file e.g. in case there are future suitable employment opportunities with BYCC, then BYCC will hold their personal data for a further 12 months after the end of the relevant recruitment exercise, or until they withdraw their consent if earlier.

Retention of data relating to members of staff: BYCC will generally hold personal data, including special categories of personal data and criminal records personal data, for the duration of a member of staff's employment or engagement.

The exceptions are:

Any personal data supplied as part of the recruitment process will not be retained if they have no bearing on the ongoing working relationship

Criminal records personal data collected in the course of the recruitment process will be deleted once they have been verified through a DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by BYCC as relevant to the ongoing working relationship

It will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by BYCC as relevant to the ongoing working relationship

If it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after six months - or once the conviction is spent, if earlier - unless information about spent convictions may be retained because the role is an excluded occupation or profession

Disciplinary, grievance and capability records will only be retained until the expiry of any warning given - but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment.

Once a member of staff has left employment - or their engagement has been terminated - BYCC will generally hold their personal data, including special categories of personal data and criminal records personal data, for 12 months after the termination of their employment or engagement, but this is subject to:

Any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records

The retention of some types of personal data for up to six years to protect against legal risk e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. BYCC will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for up to six years after the termination of their employment or engagement.

Overall, this means that BYCC will thin the file of personal data that is held on members of staff 12 months after the termination of their employment or engagement, so that BYCC only continue to retain for a longer period what is strictly necessary.

Retention of data relating to other third parties, including clients, customers and suppliers: BYCC will generally hold personal data, including special categories of personal data and criminal records personal data, belonging to clients, customers and suppliers for the duration of BYCC's business relationship with them.

Once BYCC's business relationship with a client, customer or supplier has been terminated, BYCC will generally hold their personal data, including special categories of personal data and criminal records personal data, for 12 months after the termination of the business relationship, but this is subject to:

Any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records

The retention of some types of personal data for up to six years to protect against legal risk e.g. if they could be relevant to a possible legal claim in a County Court or High Court.

Overall, this means that BYCC will thin the file of personal data that is held on clients, customers and suppliers 12 months after the termination of the business relationship, so that BYCC only continue to retain for a longer period what is strictly necessary.

Destruction and erasure: All personal data, including special categories of personal data and criminal records personal data, must be reviewed before destruction or erasure to determine whether there are special factors that mean destruction or erasure should be delayed. Otherwise, they must be destroyed or erased at the end of the retention periods outlined above. If you are responsible for maintaining personal data and are not clear what retention period should apply to a particular record, please contact BYCC's **Data Compliance Manager** for guidance.

Personal data which are no longer to be retained will be permanently erased from BYCC's IT systems or securely and effectively destroyed e.g. by cross-shredding of hard copy documents, burning them or placing them in confidential waste bins or by physical destruction of storage media, and BYCC will also require third parties to destroy or erase such personal data where applicable. You must take all reasonable steps to destroy or erase personal data that BYCC no longer require.

In some circumstances BYCC may anonymise personal data so that they no longer permit a data subject's identification. In this case, BYCC may retain such personal data for a longer period.

Pre-ticked boxes, inactivity or silence do not constitute consent.

If consent is given in a document that also deals with other matters, the request for consent must be clearly distinguishable and kept separate from those other matters. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, so you must ensure that you obtain separate consents for different types of processing, where appropriate. Data subjects also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

A clear record must be kept of all consents, including explicit consents, which covers what the data subject has consented to, what they were told at the time and how and when consent was given. This enables BYCC to demonstrate compliance with the data protection requirements for consent.

Transparency: Under the data protection legislation, the transparency principle requires BYCC to provide specific information to data subjects through appropriate privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. Privacy notices may comprise general privacy statements applicable to a specific group of data subjects e.g. youth club member, employees, volunteers or they may be stand-alone privacy statements covering processing related to a specific purpose.

BYCC must issue a privacy notice, which can be by electronic means, when BYCC first collect a data subject's personal data from them. If the personal data have been obtained from third parties, BYCC must provide the privacy notice information within a reasonable period of having obtained the personal data, but at the latest **within one month**. However, if the personal data are to be used to communicate with the data subject, the privacy notice information is to be provided, at the latest, when the first communication takes place, or if disclosure of the personal data to another recipient is envisaged, it is to be provided, at the latest, when the data are first disclosed. You must comply with these rules on privacy notices when processing personal data on BYCC's behalf in the proper performance of your job duties and responsibilities. The Trust will issue privacy notices to you from time to time.

Privacy notices can also be obtained from BYCC's Data Compliance Manager.

Accuracy:

Personal data must be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

It is important that the personal data BYCC hold about you as a data subject is accurate and up to date. Please keep BYCC informed if your personal data changes e.g. you change your home address, so that BYCC's records can be updated. BYCC cannot be held responsible for any errors in your personal data in this regard unless you have notified BYCC of the relevant change. BYCC will promptly update your personal data if you advise the organisation that the information has changed or is inaccurate. You must also ensure that the personal data that BYCC hold about other data subjects is accurate and up to date where this is part of your job duties or responsibilities. This includes special categories of personal data and criminal records personal data. You must check the accuracy of any personal data at the point of their collection and at regular intervals thereafter. You must take all reasonable steps to destroy, erase or update outdated personal data and to correct inaccurate personal data.

Integrity and confidentiality:

- Personal data must be 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.
- BYCC takes the security of personal data seriously and has implemented and maintained safeguards which are appropriate to the size and scope of the business, the amount of personal data that BYCC hold and any identified risks. This includes encryption and pseudonymisation of personal data where appropriate. BYCC have also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of BYCC's processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner. BYCC regularly test and evaluate the effectiveness of its technical and organisational safeguards to ensure the security of BYCC processing activities.
- You may only share personal data with other members of BYCC staff if they have a business need to know in order to properly perform their job duties and responsibilities.
- Hard copy personnel files, which hold personal data gathered during the working relationship, are confidential and must be stored in locked filing cabinets. Only authorised members of staff, who have a business, need to know in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets or locked drawers and cupboards when not in use by authorised members of staff. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised members of staff have access to those data.
- BYCC has local secure computers with backups in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.
- The data protection legislation requires BYCC to notify any personal data breach to the Information Commissioner's Office **within 72 hours** after becoming aware of the breach and, where there is a high risk to the rights and freedoms of data subjects, to the data subject themselves. A personal data breach is any breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and includes any act or omission that compromises

the confidentiality, integrity or availability of personal data or the safeguards that BYCC, or BYCC's third-party service providers, have put in place to protect them. BYCC has procedures in place to deal with any suspected personal data breach and you are required to comply with these. If you know or suspect that a personal data breach has occurred, you must immediately contact BYCC's **Data Compliance Manager**, retain any evidence you have in relation to the breach and follow the Trust's data breach policy and response plan. Where unlawful activity is suspected, BYCC will report the matter to the Information Commissioner's Office for investigation into the alleged breach of the data protection legislation and this may result in criminal proceedings being instigated against you. BYCC may also need to report the alleged breach to a regulatory body. This conduct would also amount to a gross misconduct offence under the Trust's disciplinary procedure and could lead to your summary dismissal.

Accountability:

BYCC is responsible for, and must be able to demonstrate compliance with, the data protection principles. This means that BYCC must implement appropriate and effective technical and organisational measures to ensure compliance and BYCC also require you to fully assist and co-operate with BYCC in this regard.

BYCC have:

A **Data Compliance Manager** who is responsible for data protection compliance and privacy matters within the business.

Keep written records of personal data processing activities

Integrated data protection requirements into BYCC internal documents, including this data protection policy, other related policies and privacy notices

Introduced a regular training program for all members of staff on the data protection legislation and on their data protection duties and responsibilities and BYCC also maintain a training record to monitor its delivery and completion - **you must undergo all mandatory data protection training**

Introduced regular reviews of BYCC privacy measures and BYCC policies, procedures and contracts and regular testing of BYCC systems and processes to monitor and assess BYCC's ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

BYCC also keep records of BYCC personal data processing activities and you are required to assist The Trust in ensuring these records are full, accurate and kept up to date.

Your obligations in relation to personal data:

You must comply with this policy and the data protection principles at all times in your personal data processing activities where you are acting on behalf of BYCC in the proper performance of your job duties and responsibilities. BYCC rely on you to help the organisation meet its data protection obligations to data subjects. Under the data protection legislation, you should also be aware that you are personally accountable for your actions and you can be held criminally liable. It is a criminal offence for you knowingly or recklessly to obtain or disclose personal data (or to procure their disclosure to a third party) without the consent of BYCC e.g. taking clients' or customers' contact details or other personal data without the Trust's consent on the termination of your employment, accessing another employee's personal data without authority or otherwise misusing or stealing personal data held by BYCC. It is also a criminal offence to knowingly or recklessly re-identify personal data that has been anonymised without the consent of BYCC, where BYCC de-identified the personal data, and it is a criminal offence to alter, block, erase, destroy or conceal personal data with the intention of preventing their disclosure to a data subject following a data subject access request.

You must also comply with the following guidelines at all times:

- Only access personal data that you have authority to access and only for authorised purposes e.g. if you need them for the work you do for BYCC, and then only use the data for the specified lawful purpose for which they were obtained
- Only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally
- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Trust's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this
- Be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request
- Where BYCC provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Trust's requirements in this regard
- Only transmit personal data between locations by e-mail if a secure network is in place e.g. encryption is used for e-mail
- If you receive a request for personal data about another member of staff or data subject, you should forward this to BYCC's **Data Compliance Manager**
- Ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with BYCC rules on computer access and secure file storage.
- Do not access another member of staff's personal data e.g. their personnel records, without authority as this will be treated as gross misconduct and it is a criminal offence
- Do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without the Trust's consent as this will be treated as gross misconduct and it is a criminal offence
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject
- Do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures (such as password protection, encryption or pseudonymisation) to secure the data and the device and it has been authorised by your line manager
- Ensure that, when working on personal data as part of your job duties and responsibilities when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- Do not store personal data on local computer drives, your own personal computer or on other personal devices
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely e.g. by cross-shredding hard copies
- Ensure that you attend all mandatory data protection training
- Refer any questions that you may have about the data protection legislation or compliance with this policy to BYCC's **Data Compliance Manager**.

Remember that compliance with the data protection legislation and the terms of this policy is your personal responsibility.

Changes to this policy: BYCC will review this policy at regular intervals and reserve the right to update or amend it at any time and from time to time. BYCC will circulate any modified policy to members of staff and, where appropriate, BYCC may notify you of changes by e-mail.

It is intended that this policy is fully compliant with the Data Protection Legislation. However, if any conflict arises between the Data Protection Legislation and this policy, BYCC will comply with the Data Protection Legislation. This policy may also be made available to the Information Commissioner's Office on request.