001 Safeguarding Policy

Date Created:	**August 2020**
Date Updated:	**October 2020**
Review Date:	**October 2021**

SAFEGUARDING IS THE RESPONSIBILITY OF EVERYBODY

Policy Statement

Black Voices Cornwall (BVC) aims to adopt the highest possible standards and take all reasonable steps in safeguarding the welfare of young people and vulnerable adults and preventing their abuse. This policy focuses on protection from abuse and neglect and is intended to support staff working within BVC. Other policies linked with this policy includes: Code of Conduct, Whistle Blowing, Complaints, Information Sharing, Grievance and Disciplinary, Safer Recruitment, Health and Safety and Equalities and Diversity.

Objectives

BVC is committed to:

- Ensuring that the welfare of children, young people and vulnerable adults is paramount at all times.
- Maximising people's choice, control and inclusion and protecting their human rights.
- Working in partnership with others agencies in order to safeguarding children, young people and vulnerable adults.
- Ensuring safe and effective working practices are in place.
- Supporting staff within the Best Practice People.

Definitions

Child, Children and Young People

In terms of this policy, "child, children and young people" mean those under the age of 18 as Defined by The Children Act 1989. This policy applies to students in this age group attending a further education course and young people aged 16 - 18 who attend courses in relation to their apprenticeships.

Vulnerable Adults

A vulnerable adult is a person aged 18 years or over who may be unable to take care of themselves or protect themselves from harm or from being exploited.

This may include a person who:

- is living in residential accommodation, such as a care home or a residential special school;
- is living in sheltered housing;
- is detained in lawful custody (in a prison, remand centre, young offender institution, secure training centre or attendance centre, or under the powers of the Immigration and Asylum Act 1999;
- is receiving domiciliary care in their own home;
- is receiving any form of healthcare;
- is under the supervision of the probation services;

- is receiving a specified welfare service, namely the provision of support, assistance or advice by any person, the purpose of which is to develop an individual's capacity to live independently in accommodation or support their capacity to do so;
- is receiving a service or participating in an activity for people who have particular needs because of their age or who have any form of disability;
- is an expectant or nursing mother living in residential care;
- is receiving direct payments from a local authority or health and social care trust in lieu of social care services, or
- requires assistance in the conduct of their own affairs.

This also applies to temporary conditions.

Staff

Staff means all employees, full-time, part-time, teaching staff, and all agency, franchise, contract and volunteer staff working for or on behalf of BVC.

Abuse

Abuse is the violation of an individual's human rights. It can be a single act or repeated acts. It can be physical, sexual, emotional or financial. It also includes acts of neglect or an omission to act. In all forms of abuse there are elements of emotional abuse. Vulnerable adults may also suffer additional types of abuse such as cuckooing, being manipulated financially or being discriminated against. Other examples of abuse include inflicting physical harm such as hitting or misuse of medication, rape and sexual assault or exposure to sexual acts without informed consent, emotional abuse such as threats, humiliation and harassment, exploitation, ignoring medical or physical needs, withholding of necessities of life such as food or heating. This list is not definitive.

Coverage

This policy applies to all staff, learners, temporary staff, part-time workers, volunteers as well as all people who work on behalf of BVC.

Nominated Safeguarding Lead

The Designated person within BVC is:

NAME Helen Hutchinson Contact number: 07738230028

Helen Hutchinson shall be made known to learners, employees and sub-contractors; as the designated person to whom concerns will be addressed. Helen is Level 3 trained in Safeguarding Multi Agency Child Protection. If the concern is about the designated person, please report to the BCT Board or use the Whistle Blowing Policy and report directly to LADO.

Responsibilities of BVC

- BVC has accepted the principles laid by the Safeguarding Vulnerable Groups Act 2006, the Children and Families Act 2014, Keeping Children Safe in Education 2020, Working Together to Safeguard Children 2017;
- To take action to identify and prevent abuse from happening;
- Respond appropriately when abuse has or is suspected to have occurred;

- Ensure that the agreed safeguarding adults and child, children and young people procedures are followed at all times;
- Provide support, advice and resources to staff in responding to safeguarding issues;
- Inform staff of any local or national issues relating to safeguarding adults and children;
- Ensure staff are aware of their responsibilities and to attend training and to support staff in accessing these events;
- Ensuring that our organisation has a dedicated staff member with an expertise in safeguarding adults and children;
- Ensuring staff have access to appropriate consultation and supervision regarding safeguarding adults and children;
- Understand how diversity, beliefs and values of people who use services may influence the identification, prevention and response to safeguarding concerns;
- Ensure that information is available for people that use services, family members setting out what to do if they have a concern;
- Ensure that all employees who come in contact with vulnerable adults and a child, children and young people have a DBS check in line with the requirements of the Independent Safeguarding Authority Vetting and Barring Scheme;
- Ensure that any adult within BVC who has a disclosure on their DBS that a Positive Disclosure Risk Assessment for the person will be carried before they are able to engage in activities with children and vulnerable adults;

Responsibilities of all members of BVC

- Follow the safeguarding policies and procedures at all times, particularly if concerns arise about the safety or welfare of a vulnerable adult, a child, children or a young person;
- Participate in safeguarding training and maintain current working knowledge;
- Discuss any concerns about the welfare of a vulnerable adult, a child, children or young people with the BVC Designated Safeguarding Lead;
- Contribute to actions required including information sharing and attending meetings;
- Work collaboratively with other agencies to safeguard and protect the welfare of people who use services;
- Remain alert at all times to the possibility of abuse;
- Recognise the impact that diversity, beliefs and values of people who use services can have.

Training

All staff should receive basic safeguarding awareness training at a level according to their role and this should be refreshed as a minimum every three years. The Designated Safeguarding Lead needs to be trained to at least Level 3 and refreshed every two years. At least One Director should hold Safer Recruitment training.

Reporting Abuse

The following procedure details the actions to be taken by both the complainant and Staff:

- If staff suspects a vulnerable person is being abused or is at risk of abuse, they are expected to report concerns to the Designated Safeguarding Lead, Helen Hutchinson (unless they suspect that the DSL is implicated – in such circumstances the whistle blowing policy should be followed);
- If at any time staff feel the person needs urgent medical assistance, they have a duty to call for an ambulance or arrange for a doctor to see the person at the earliest opportunity;
- If at the time staff have reason to believe the vulnerable person is in immediate and serious risk of harm or that a crime has been committed the police must be called or contact the Multi Agency Referral Unit (MARU) (0300 1231 116);
- A report form must be completed where there are allegations of abuse and sent to the DSL;
- All service users/learners need to be safe. Throughout the process the service users/learners needs remain paramount. This process is about protecting the vulnerable adults, children and young people and prevention of abuse;
- Reporting Safeguarding incident takes priority over everything else.

Alleged abuser and victims who are both service users/learners

It is important that consideration be given to a co-ordinated approach and partnership working, where it is identified that both the alleged abuser and alleged victim are service users/learners.

Where both parties are receiving a service staff should discuss cases and work together. Meetings with both the alleged abuser and alleged victim in attendance may not be considered appropriate.

Allegation of abuse staff member

Employees should be aware that abuse is a serious matter that can lead to a criminal conviction. Where applicable the disciplinary policy of BVC will be implemented.

Confidentiality and information sharing

It is important to identify an abusive situation as early as possible so that the individual can be protected. Withholding information may lead to abuse not being dealt with in a timely manner. Confidentiality must never be confused with secrecy. The Staff has a duty to share information relating to suspected abuse and the DSL of BVC will decide whether to refer the case to the relevant body (e.g. MARU, Social Services, the Police)

Consent is not required to breach confidentiality (capacity issues must be considered) and make a safeguarding referral where;

- A serious crime has been committed;
- Where the alleged perpetrator may go on to abuse others;
- Other vulnerable adults are at risk in some way;
- The vulnerable adult, child, children and young person is deemed to be in serious risk;
- There is a statutory requirement e.g. Safeguarding Vulnerable Groups Act 2006, Children's Act 2004, Mental Health Act 1983, Care Standards Act 2000;

- The public interest overrides the interest of the individual;
- When a member of staff of a statutory service, a private or voluntary service or a volunteer is the person accused of abuse, malpractice or poor professional standards.

If a worker has any doubt about the legality of sharing information, they must in the first instance consult the DSL dealing with safeguarding issues.

Monitoring. This policy will be reviewed annually by the Assurance Board.

APPENDICIES TAKEN FROM THE MAIN CORNWALL COUNCIL SAFEGUARDING POLICY

Appendix A: Signs and Indicators of Abuse

A more comprehensive list will be considered within staff training however this will give staff some indication of what to look out for.

Although these signs do not necessarily indicate that a child has been abused, they may help staff recognise that something is wrong.

If you have any concerns you must pass these to your DSL immediately.

Physical Abuse

Most children will collect cuts and bruises and injuries, and these should always be interpreted in the context of the child's medical / social history, developmental stage and the explanation given. Most accidental bruises are seen over bony parts of the body, e.g. elbows, knees, shins, and are often on the front of the body. Some children, however, will have bruising that is more than likely inflicted rather than accidental.

Important indicators of physical abuse are bruises or injuries that are either unexplained or inconsistent with the explanation given; these can often be visible on the 'soft' parts of the body where accidental injuries are unlikely, e g, cheeks, abdomen, back and buttocks. Occasionally a 'pattern' may be seen e.g. fingertip or hand mark. A delay in seeking medical treatment when it is obviously necessary is also a cause for concern.

The physical signs of abuse may include:

- Unexplained bruising, marks or injuries on any part of the body.
- Multiple bruises- in clusters, often on the upper arm, outside of the thigh.
- Cigarette burns.
- Human bite marks.
- Broken bones.
- Burns- shape of burn, uncommon sites, friction burn

Changes in behaviour that can also indicate physical abuse:

- Fear of parents being approached for an explanation.
- Aggressive behaviour or severe temper outbursts.
- Flinching when approached or touched.
- Reluctance to get changed, for example in hot weather.
- Depression.
- Withdrawn behaviour.
- Running away from home.

Neglect

It can be difficult to recognise neglect; however, its effects can be long term and damaging for children.
It is also impossible to recognize that aspects of neglect can be very subjective. We may need to challenge ourselves and others and remember that people can have different values and that there will be differences in how children are cared for which may be based on faith or cultural issues that our different to ours.

In respecting these differences, we must not be afraid to raise our concerns if we believe the care being given to the child may be impacting on its safety and welfare.

The physical signs of neglect may include:

- Being constantly dirty or 'smelly'.
- Constant hunger, sometimes stealing food from other children.
- Losing weight or being constantly underweight (obesity may be a neglect issue as well).
- Inappropriate or dirty clothing

Neglect may be indicated by changes in behaviour which may include:

- Mentioning being left alone or unsupervised.
- Not having many friends.
- Complaining of being tired all the time.
- Not requesting medical assistance and/or failing to attend appointments

Emotional Abuse

Emotional abuse can be difficult to identify as there are often no outward physical signs. Indications may be a developmental delay due to a failure to thrive **(also known as faltering growth**) and grow, however, children who appear well-cared for may nevertheless be emotionally abused by being taunted, put down or belittled. They may receive little or no love, affection or attention from their parents or carers. Emotional abuse can also take the form of children not being allowed to mix or play with other children.

Changes in behaviour which can indicate emotional abuse include:

- Neurotic/anxious behaviour e.g. sulking, hair twisting, rocking.
- Being unable to play.
- Fear of making mistakes.
- Sudden speech disorders.
- Self-harm.
- Fear of parent being approached regarding their behaviour.
- Development delay in terms of emotional progress.
- Overreaction to mistakes.

Sexual Abuse

It is recognised that there is underreporting of sexual abuse within the family. All Staff and Governors should play a crucial role in identifying / reporting any concerns that they may have through, for example, the observation and play of younger children and understanding the indicators of behaviour in older children which may be underlining of such abuse.

All Staff and Governors should be aware that adults, who may be men, women or other children, who use children to meet their own sexual needs abuse both girls and boys of all ages. Indications of sexual abuse may be physical or from the child's behaviour. In all cases, children who tell about sexual abuse do so because they want it to stop. It is important, therefore, that they are listened to and taken seriously.

The physical signs of sexual abuse may include:

- Pain or itching in the genital area.
- Bruising or bleeding near genital area.
- Sexually transmitted disease.
- Stomach pains
- Discomfort when walking or sitting down.

Changes in behaviour which can also indicate sexual abuse include:

- Sudden or unexplained changes in behaviour e.g. becoming aggressive or withdrawn.
- Fear of being left with a specific person or group of people.
- Sexual knowledge which is beyond their age, or developmental level.
- Sexual drawings or language.
- Eating problems such as overeating or anorexia.
- Self-harm or mutilation, sometimes leading to suicide attempts. · Saying they have secrets they cannot tell anyone about · Acting in a sexually explicit way towards adults.

Note: A child may be subjected to a combination of different kinds of abuse. It is also possible that a child may show no outward signs and hide what is happening from everyone.

Child Sexual Exploitation (CSE)

Many aspects of CSE take place online so it may be difficult to identify this within school. **The behaviours also need to be considered within the context of the child's age and stage of development. As they get older this may be more difficult to identify. However, abuse indicators may include:**

- Children talking about having lots of 'friends' online whom when asked the do not know personally
- Disengagement from education
- Using drugs or alcohol
- Unexplained gifts/money
- Repeat concerns about sexual health
- Decline in emotional wellbeing
- Talking about physically meeting up with someone they met online
- Posting lots of images of themselves online
- Going missing
- Talking about friendships with older young people/adults
- Engagement with offending
- Exclusion or unexplained absences from school
- Isolation from peers/social network
- Frequently in the company of older people – association with 'risky' adults
- Accepting lifts or being picked up in vehicles
- Physical injury without plausible explanation
- No parental supervision/monitoring of online activity
- Poor school attendance
- Secretive behaviour
- Self-harm or significant changes in emotional well-being
- Concerning use of internet or other social media
- Returning home late
- Chronic tiredness

Female Genital Mutilation (FGM)

Although situations of FGM may be unusual it is important that you do not assume it could not happen here. **8- 15-year-old girls are the most vulnerable**

Indicators may include:

- Days absent from school
- Not participating in physical education
- In pain/has restricted movement/frequent and long visits to the toilet/broken limbs
- Confides that she is having a special procedure, cut or celebration
- Unauthorised and or extended leave, vague explanations or plans for removal of a female in a high-risk category especially over the summer period
- Plans to take a holiday which may be unauthorised, unexplained or extended in a country known to practice FGM
- Parents from a country who are known to practice FGM.

Appendix B: Dealing with a Disclosure of Abuse

It is extremely important that if a child discloses that you know what to do. This will be explained by the DSL/DDSL during induction and will form a key part of any safeguarding training undertaken within school. These are the key principles:

If:

- A child or young person discloses abuse, or
- You suspect a child may have been abused, or
- You witness an abusive situation involving another professional.

You **RECORD AND REPORT:**

- Respond without showing any signs of disquiet, anxiety or shock.
- Enquire casually about how an injury was sustained or why a child appears upset.

  E.g. How did you .....?
- Confidentiality must never be promised to children, young people, or adults in this situation.
- Observe carefully the demeanour or behaviour of the child.
- Record in detail what has been seen and heard in the child's own words (after you have spoken to them, not during a disclosure).
- Do not interrogate or enter into detailed investigations**:** rather, encourage the child to say what **she/** he wants until enough information is gained to decide whether or not a referral is appropriate.
- Ensure if the child is complaining of being hurt/unwell this is reported immediately

  Asking questions is fine to help understand what the issue is BUT you must ensure the questions are open and give the child the ability to clarify.
- It is important NOT to ask leading questions e.g. Did ----- Was it ------**?**.
- It is important to know when to stop asking questions and listen.
- It is important not to interrogate**.**
-

Types of Questions you can ask:

· Tell me? (tell me what happened)
· Explain? (explain what you meant by)
· Where did this happen/where were you? · When did this happen?

Remember you are only clarifying with the child if something concerning did happen or could have happened from the information, they give you.

Then report to your DSL or DDSL immediately.

Staff **MUST NOT**

- Investigate suspected/alleged abuse themselves;
- Evaluate the grounds for concern;
- Seek or wait for proof;
- Discuss the matter with anyone other than the designated staff or MARU;
- Speak to the parents until you have had a conversation with your DSL/MARU;
- Ask the child to repeat the information to anyone including the DSL/DDSL;
- Promise to keep it a secret.

Appendix C

Key Documents:

This is an overarching policy and should be read in conjunction with the following documents:

'Working Together to Safeguard Children' 2018

The guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779401/Working_Together_to_Safeguard-Children.pdf

"Keeping Children Safe in Education" 2020,

The guidance is available via the following link:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912592/Keeping_children_safe_in_education_Sep_2020.pdf

'What to do if worried a child is being Abused: Advice for Practitioner'. March 2015.

The guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779401/Working_Together_to_Safeguard-Children.pdf

"Information Sharing: Advice for Practitioners providing Safeguarding Services to Children, Young People, Parents and Carers". 2018.

The guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

"The Prevent Duty Departmental, advice for Schools and childcare providers June 2015.

The guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Multi agency Statutory Guidance on Female Genital Mutilation (pages 59-61 focus on schools).

The guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912996/6-1914-HO-Multi_Agency_Statutory_Guidance_on_FGM__-_MASTER_V7_-_FINAL__July_2020.pdf

Children Missing Education- Statutory guidance for local authorities. September 2016.

The guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550416/Children_Missing_Education_-_statutory_guidance.pdf

Multi agency Statutory Guidance for dealing with Forced Marriage July 2014:

This guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/322310/HMG_Statutory_Guidance_publication_180614_Final.pdf

Child Sexual Exploitation

Further guidance is available via the following link:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591903/CSE_Guidance_Core_Document_13.02.2017.pdf

Child Sexual Exploitation Definition and a guide for Practitioners DOE February 2017

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591905/CSE_Guidance_Annexes_13.02.2017.pdf

Guidance for Safer Working Practice for those working with Children and Young People in Education settings 2015.

This guidance is available via the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912592/Keeping_children_safe_in_education_Sep_2020.pdf

Additional information has been included from Somerset County Council Exemplar Safeguarding Policy (September 2016) and Derbyshire County Council Exemplar Safeguarding Policy (October 2016).

Appendix D

Specific Safeguarding Issues:

There are specific issues that have become critical issues in Safeguarding that it is good to be aware of:

- Bullying including cyber bullying
- Child Sexual Exploitation (CSE)
- Children missing & out of Education (CMOE/CME)
- Reduced timetables
- Exclusions
- Domestic Violence
- Drugs
- Fabricated or induced illness
- Faith abuse
- Female Genital Mutilation (FGM)
- Forced Marriage
- Gangs and Youth Violence
- Gender based violence/Violence against women and girls (VAWG)
- Hate
- Mental Health
- Private Fostering
- Preventing Radicalisation
- Online abuse/Sexting
- Teenage Relationship abuse
- Trafficking
- Missing children and vulnerable adults
- Child sexual abuse within the family
- Poor parenting, particularly in relation to babies and young children
- Cuckooing
- County Lines
- Financial Abuse
- Coercive Control

BLACK VOICES CORNWALL

002 WHISTLE BLOWING POLICY

Date Created:	August 2020
Date Updated:	October 2020
Review Date:	October 2021

Staff and volunteers may be the first to realise that there is something seriously wrong within BVC. However, they may be unsure about expressing their concerns because they are worried about being disloyal to colleagues or BVC. Whistleblowing encourages and enables staff to raise serious concerns within BVC.

BVC's Commitment

BVC is committed to openness and accountability. BVC expects staff, volunteers, and others that we deal with, to voice any serious concerns about any aspect of our work.

BVC's Whistleblowing Policy aims to:

- enable you to raise concerns in confidence and receive feedback on action taken;
- ensure you receive a response to your concerns and that you are aware of how to pursue them if you are not satisfied;
- reassure you that you will be protected from possible reprisals or victimisation if you have a reasonable belief that you have made a disclosure in good faith.

What Type of Concerns are Covered?

- Conduct which is a an offence or breach of law;
- Disclosure related to miscarriages of justice;
- Health and safety risks, including risks to the public as well as other staff or volunteers;
- Damage to the environment;
- Unauthorised use of public funds;
- Possible fraud or corruption;
- Sexual, physical, emotional or financial abuse of service users;
- Other unethical conduct.

Safeguards

BVC recognises that the decision to report a concern can be difficult. If what you are saying is true, you should have nothing to fear because you will be doing your duty. Black Voices Cornwall will make every effort to ensure anyone reporting a concern is safeguarded and supported to do so.

Reporting

Whistleblowing can be reported to your supervisor or a member of the Executive Board, Local Authority Designated Officer (LADO), Police 101 or in cases of emergency 999.

BVC also follows the guidance provided by Department for Business, Innovation and Skills

003
Privacy Policy

Date Created:	**February 2021**
Date Updated:	**February 2021**
Review Date:	**October 2021**

PRIVACY POLICY

BACKGROUND:

Black Voices Cornwall understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of everyone who visits this website, www.blackvoicescornwall.org and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

Please read this Privacy Policy carefully and ensure that you understand it. Your acceptance of this Privacy Policy is requested is upon visiting this website and any subsequent visits.

1. **Definitions and Interpretation**

In this Policy the following terms shall have the following meanings:

"Account"	means an account required to access and/or use certain areas and features of our site;
"Cookie"	means a small text file placed on your computer or device by **our** Site when you visit certain parts of **our** Site and/or when you use certain features of our Site. Details of the Cookies used by **our** Site are set out in Part 14, below; and
["Cookie Law"	means the relevant parts of the Privacy and Electronic Communications (EC Directive) Regulations 2003;**]**

2. **Information About Us**

Our Site is owned and operated by Black Voices Cornwall, a limited company, 12820882

Registered address: C-Space, 5-7 The Crescent Newquay, Cornwall

Data Protection Officer: Marcus Alleyne.

Email address: info@blackvoicescornwall.org.

Telephone number: 07891001969.

Postal address: C-Space, 5-7 The Crescent Newquay, Cornwall

We are regulated by Black Voices Cornwall Assurance Board

3. What Does This Policy Cover?

This Privacy Policy applies only to your use of **[**Our**]** Site. **[**Our**]** Site may contain links to other websites. Please note that **[**we**]** have no control over how your data is collected, stored, or used by other websites and **[**we**]** advise you to check the privacy policies of any such websites before providing any data to them.

4. What Is Personal Data?

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "GDPR") and the Data Protection Act 2018 (collectively, "the Data Protection Legislation") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

5. What Are My Rights?

Under the Data Protection Legislation, you have the following rights, which **[**we**]** will always work to uphold:

a) The right to be informed about **[**our**]** collection and use of your personal data. This Privacy Policy should tell you everything you need to know, but you can always contact **[**us**]** to find out more or to ask any questions using the details in Part 15.

b) The right to access the personal data **[**we**]** hold about you. Part 13 will tell you how to do this.

c) The right to have your personal data rectified if any of your personal data held by **[**us**]** is inaccurate or incomplete. Please contact **[**us**]** using the details in Part 15 to find out more.

d) The right to be forgotten, i.e. the right to ask **[**us**]** to delete or otherwise dispose of any of your personal data that **[**we**]** hold. Please contact **[**us**]** using the details in Part 15 to find out more.

e) The right to restrict (i.e. prevent) the processing of your personal data.

f) The right to object to **us** using your personal data for a particular purpose or purposes.

g) The right to withdraw consent. This means that, if **[**we are**]** relying on your consent as the legal basis for using your personal data, you are free to withdraw that consent at any time.

h) The right to data portability. This means that, if you have provided personal data to **[**us**]** directly, **[**we are**]** using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask **[**us**]** for a copy of that personal data to re-use with another service or business in many cases.

i) Rights relating to automated decision-making and profiling. **[**We**]** do not use your personal data in this way.**]**

For more information about **[**our**]** use of your personal data or exercising your rights as outlined above, please contact **[**us**]** using the details provided in Part 15.

It is important that your personal data is kept accurate and up-to-date. If any of the personal data **[**we**]** hold about you changes, please keep **[**us**]** informed as long as **[**we**]** have that

data.

Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If you have any cause for complaint about **[**our**]** use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office. **[**We**]** would welcome the opportunity to resolve your concerns **[**ourselves**]** however, so please contact **[**us**]** first, using the details in Part 15.

6. What Data Do You Collect and How?

Depending upon your use of **[**Our**]** Site, **[**we**]** may collect and hold some or all of the personal **[**and non-personal**]** data set out in the table below, using the methods also set out in the table. Please also see Part 14 for more information about **[**our**]** use of Cookies and similar technologies **[**and **[**our**]** Cookie Policy. **[**We**]** do not collect any 'special category' or 'sensitive' personal data**]** **AND/OR** **[**personal data relating to children **OR** **[**data relating to criminal convictions and/or offences**]**.

Data Collected	How [We] OR [I] Collect the Data
Identity Information including name, title, date of birth, gender, ethnicity	Website data collection, email correspondence, mailing list
Contact information including address, email address, telephone number	Website data collection, email correspondence, mailing list
[Business information including <<insert data collected, e.g. business name, job title, profession>>.**]**	Website data collection, email correspondence, mailing list
[Payment information including <<insert data collected, e.g. card details, bank account numbe	Website data collection, email correspondence, mailing list
Profile information including, preferences, interests, login details, purchase history	Website data collection, email correspondence, mailing list ethod of collection and/or so
Technical information including IP address, browser type and version, operating system	Website data collection, email correspondence, mailing list
[Data from third parties including technical information, contact information, profile information	Website data collection, email correspondence, mailing list

7. How Do You Use My Personal Data?

Under the Data Protection Legislation, **[**we**]** **OR** **[**I**]** must always have a lawful basis for using personal data. The following table describes how **[**we**]** **OR** **[**I**]** **[**will**]** **OR** **[**may**]** use your personal data, and **[**our**]** **OR** **[**my**]** lawful bases for doing so:

What We Do	Name, geographic location, age, gender, ethnicity	Our Lawful Basis
[Registering you on	Name, geographic location, age, gender, ethnicity	

Providing and managing your Account.	Name, geographic location, age, gender, ethnicity	legitimate interests, training and development
	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)
Personalising and tailoring your experience on Our Site.	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

Administering Our Site.	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)
Administering our business.	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

Supplying our products **AND** services to you.	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)
Managing payments for our products **OR** services	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

Personalising and tailoring our **OR** products **OR** services for you	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)
Communicating with you.	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

Supplying you with information by email **OR** post that you have opted-in-to (you may opt-out at any time by unsubscribing or contacting the organisation at the above address.	Name, geographic location, age, gender, ethnicity	Consent of the data subject Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract Processing is necessary for compliance with a legal obligation Processing is necessary to protect the vital interests of a data subject or another person Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

With your permission and/or where permitted by law, we may also use your personal data for marketing purposes, which may include contacting you by email **AND/OR** telephone **AND/OR** text message **AND/OR** post with information, news, and offers on our products **AND/OR** services. You will not be sent any unlawful marketing or spam. We will always work to fully protect your rights and comply with our obligations under the Data Protection Legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and you will always have the opportunity to opt-out. We will always obtain your express opt-in consent before sharing your personal data with third parties for marketing purposes and you will be able to opt-out at any time.

We will only use your personal data for the purpose(s) for which it was originally collected unless we reasonably believe that another purpose is compatible with that or those original purpose(s) and need to use your personal data for that purpose. If we do use your personal data in this way and you wish us to explain how the new purpose is compatible with the original, please contact us using the details in Part 15.

If we need to use your personal data for a purpose that is unrelated to, or incompatible with, the purpose(s) for which it was originally collected, we will inform you and explain the legal basis which allows us to do so.

In some circumstances, where permitted or required by law, we may process your personal data without your knowledge or consent. This will only be done within the bounds of the Data Protection Legislation and your legal rights.

8. How Long Will You Keep My Personal Data?

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept for the following periods (or, where there is no fixed period, the following factors will be used to determine how long it is kept):

Type of Data	How Long We Keep It
Identity Information including name, title, date of birth, gender, ethnicity	Until BVC ceases operation or data removal request is made
Contact information including address, email address, telephone number	Until BVC ceases operation or data removal request is made
Business information includingbusiness name, job title, profession	Until BVC ceases operation or data removal request is made
Payment information including card details, bank account numbers	Until BVC ceases operation or data removal request is made
Profile information including preferences and interests, username and password, purchase history	Until BVC ceases operation or data removal request is made
Technical information including IP address, browser type and version, operating system	Until BVC ceases operation or data removal request is made

9. **How and Where Do You Store or Transfer My Personal Data?**

We will only store or transfer your personal data **OR** store or transfer some of your personal data within the UK. This means that it will be fully protected under the Data Protection Legislation.

10. **Do You Share My Personal Data?**

We will not share any of your personal data with any third parties for any purposes, subject to the following exception**[**s**]**.

If we sell, transfer, or merge parts of our business or assets, your personal data may be transferred to a third party. Any new owner of our business may continue to use your personal data in the same way(s) that we have used it, as specified in this Privacy Policy.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

If any of your personal data is shared with a third party, as described above, we will take steps to ensure that your personal data is handled safely, securely, and in accordance with your rights, our obligations, and the third party's obligations under the law, as described above in Part 9.**]**

If any personal data is transferred outside of the EEA, we will take suitable steps in order to ensure that your personal data is treated just as safely and securely as it would be within the UK and under the Data Protection Legislation, as explained above in Part 9.

If we sell, transfer, or merge parts of our business or assets, your personal data may be transferred to a third party. Any new owner of our business may continue to use your personal data in the same way(s) that we have used it, as specified in this Privacy Policy.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

11. **How Can I Control My Personal Data?**

1. In addition to your rights under the Data Protection Legislation, set out in Part 5, when you submit personal data via Our Site, you may be given options to restrict our

use of your personal data. In particular, we aim to give you strong controls on our use of your data for direct marketing purposes (including the ability to opt-out of receiving emails from us which you may do by unsubscribing using the links provided in our emails and at the point of providing your details .

2. You may also wish to sign up to one or more of the preference services operating in the UK: The Telephone Preference Service ("the TPS"), the Corporate Telephone Preference Service ("the CTPS"), and the Mailing Preference Service ("the MPS"). These may help to prevent you receiving unsolicited marketing. Please note, however, that these services will not prevent you from receiving marketing communications that you have consented to receiving.

12. Can I Withhold Information?

You may access certain areas of Our Site without providing any personal data at all. However, to use all features and functions available on Our Site you may be required to submit or allow for the collection of certain data.

You may restrict our use of Cookies. For more information, see Part 14

13. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request".

All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 15.

There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within **15 working days** and, in any case, not more than one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

14. How Do You Use Cookies?

Our Site may place and access certain first-party Cookies on your computer or device. First-party Cookies are those placed directly by us and are used only by us. We use Cookies to facilitate and improve your experience of **[**Our**] OR [**My**]** Site and to provide and improve our products and services. We have carefully chosen these Cookies and have taken steps to ensure that your privacy and personal data is protected and respected at all times.

By using Our Site, you may also receive certain third-party Cookies on your computer or device. Third-party Cookies are those placed by websites, services, and/or parties other than us. Third-party Cookies are used on Our Site for data and impact analysis. These Cookies are not integral to the functioning of Our Site and your use and experience of Our Site will not be impaired by refusing consent to them.

All Cookies used by and on Our Site are used in accordance with current Cookie Law.

Before Cookies are placed on your computer or device, you will be shown a pop up prompt requesting your consent to set those Cookies. By giving your consent to the placing of Cookies you are enabling us to provide the best possible experience and service to you. You may, if you wish, deny consent to the placing of Cookies; however certain features of Our Site may not function fully or as intended.

Our Site uses analytics services provided by website.com. Website analytics refers to a set of tools used to collect and analyse anonymous usage information, enabling us to better understand how Our Site is used. This, in turn, enables us to improve Our Site and the products **AND** services offered through it.

The analytics service(s) used by Our Site use(s) Cookies to gather the required information. You do not have to allow us to use these Cookies, however whilst our use of them does not pose any risk to your privacy or your safe use of Our Site, it does enable us to continually improve Our Site, making it a better and more useful experience for you.

In addition to the controls that we provide, you can choose to enable or disable Cookies in your internet browser. Most internet browsers also enable you to choose whether you wish to disable all Cookies or only third-party Cookies. By default, most internet browsers accept Cookies, but this can be changed. For further details, please consult the help menu in your internet browser or the documentation that came with your device.

You can choose to delete Cookies on your computer or device at any time, however you may lose any information that enables you to access Our Site more quickly and efficiently including, but not limited to, login and personalisation settings.

It is recommended that you keep your internet browser and operating system up-to-date and that you consult the help and guidance provided by the developer of your internet browser and manufacturer of your computer or device if you are unsure about adjusting your privacy settings.**]**

15. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details (for the attention of Marcus Alleyne):

Email address: info@blackvoicescornwall.org

Telephone number: 07891001969

Postal Address: C-Space, 7-5 The Crescent, Newquay, Cornwall

16. Changes to this Privacy Policy

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Any changes will be immediately posted on Our Site and you will be deemed to have accepted the terms of the Privacy Policy on your first use of Our Site following the alterations. We recommend that you check this page regularly to keep up-to-date. This Privacy Policy was last updated on 10th February 2021.

004
Data Protection Policy

Date Created:	**August 2020**
Date Updated:	**February 2021**
Review Date:	**October 2021**

1. Introduction

This Policy sets out the obligations of Black Voices Cornwall (BVC) , a company registered in England under number 12820882, whose registered office is at 5-7 The Crescent, Newquay Cornwall (BVC) regarding data protection of staff, customers, business contacts and partners in respect of their personal data under Data Protection Law (all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, EU Regulation 2016/679 General Data Protection Regulation ("GDPR"), the Data Protection Act 2018, and any successor legislation or other directly applicable EU regulation relating to data protection and privacy for as long as, and to the extent that, EU law has legal effect in the UK).

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Definitions

"consent"	means the consent of the data subject which must be a 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;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to <<insert type(s) of data subject, e.g. staff, customers, business contacts etc.>> used in our business for our commercial purposes;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom the Company holds personal data;

"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. **Scope**

1. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.
2. The Company's Data Protection Officer is Marcus Alleyne. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
3. All directors, managers, department heads, supervisors and volunteers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

4. Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

   a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

   b) if consent is being relied upon in order to collect, hold, and/or process personal data;

   c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

   d) if any new or amended privacy notices or similar privacy-related documentation are required;

   e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

   f) if a personal data breach (suspected or actual) has occurred;

   g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

   h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

   i) if personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so;

   j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

   k) when personal data is to be used for purposes different to those for which it was originally collected;

   l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

   m) if any assistance is required in complying with the law applicable to direct marketing.

4. The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

1. processed lawfully, fairly, and in a transparent manner in relation to the data subject;
2. 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;
3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
4. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the data subject;

6. 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.

5. The Rights of Data Subjects

The GDPR sets out the following key rights applicable to data subjects:

1. The right to be informed;
2. the right of access;
3. the right to rectification;
4. the right to erasure (also known as the 'right to be forgotten');
5. the right to restrict processing;
6. the right to data portability;
7. the right to object; and
8. rights with respect to automated decision-making and profiling.

6. Lawful, Fair, and Transparent Data Processing

1. Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful if at least one of the following applies:

   a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

   b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

   c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

   d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

   e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

   f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. **[**If the personal data in question is special category personal data (also known as "sensitive personal data"), at least one of the following conditions must be met:

   a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

   b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as

it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

e) the processing relates to personal data which is manifestly made public by the data subject;

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

g) the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.**]**

7. **Consent**

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

1. Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

2. Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

3. Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

4. If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

5. If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

6. In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

1. The Company collects and processes the personal data set out in Part 24 of this Policy. This includes:

   a) personal data collected directly from data subjects **and**

   b) **[**personal data obtained from third parties.**]**

2. The Company only collects, processes, and holds personal data for the specific purposes set out in Part 24 of this Policy (or for other purposes expressly permitted by the GDPR).

3. Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

9. Adequate, Relevant, and Limited Data Processing

1. The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 24, below.

2. Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

3. Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

10. Accuracy of Data and Keeping Data Up-to-Date

1. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17, below.

2. The accuracy of personal data shall be checked when it is collected and at **[**regular**] OR [**<<insert interval>>**]** intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. **Data Retention**

1. The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
3. For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

12. **Secure Processing**

1. The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 25 to 30 of this Policy.
2. All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
3. Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:
    a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;
    b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
    c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

13. **Accountability and Record-Keeping**

1. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
2. The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).
3. All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.
4. The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.
5. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
    1. the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
    2. the purposes for which the Company collects, holds, and processes personal data;

3. the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;
4. details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
5. details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
6. details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);
7. details of personal data storage, including location(s);
8. detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

14. Data Protection Impact Assessments and Privacy by Design

1. In accordance with the privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.
2. The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:
   a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
   b) the state of the art of all relevant technical and organisational measures to be taken;
   c) the cost of implementing such measures; and
   d) the risks posed to data subjects and to the Company, including their likelihood and severity.
3. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
   a) the type(s) of personal data that will be collected, held, and processed;
   b) the purpose(s) for which personal data is to be used;
   c) the Company's objectives;
   d) how personal data is to be used;
   e) the parties (internal and/or external) who are to be consulted;
   f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
   g) risks posed to data subjects;
   h) risks posed both within and to the Company; and
   i) proposed measures to minimise and handle identified risks.

15. Keeping Data Subjects Informed

1. The Company shall provide the information set out in Part 15.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

2. The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 24 of this Policy) and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place (see Part 31 of this Policy for further details);

g) details of applicable data retention periods;

h) details of the data subject's rights under the GDPR;

i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. **Data Subject Access**

1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

2. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at <<insert contact details>>.

3. Responses to SARs must normally be made within one month of receipt, however,

this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

4. All SARs received shall be handled by the Company's Data Protection Officer.

5. The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. **Rectification of Personal Data**

1. Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

2. The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. **Erasure of Personal Data**

1. Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

   a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

   b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

   c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

   d) the personal data has been processed unlawfully;

   e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation.

   f) the personal data is being held and processed for the purpose of providing information society services to a child.

2. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

3. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. **Restriction of Personal Data Processing**

1. Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain

only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. **Data Portability**

1. The Company processes personal data using automated means.

2. Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

3. To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format**[**s**]**:

   a) Digital format

   b) Hard paper copy upon request.

4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

5. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

21. **Objections to Personal Data Processing**

1. Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

2. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

3. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

4. **[**Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

22. **[Automated Processing, Automated Decision-Making, and Profiling**

1. ~~The Company uses no personal data in automated decision-making processes as follows:~~

   a) ~~inclusion on mailing list~~

2. **[**~~The Company uses personal data for profiling purposes as follows:~~

   a)

3. The activities described in this Part 22 are generally prohibited under Data Protection Law where the resulting decisions have a legal or similarly significant

effect on data subjects unless one of the following applies:

a) the data subject has given their explicit consent;

b) the processing is authorised by law; or

c) the processing is necessary for the entry into, or performance of, a contract between the Company and the data subject.

4. If special category personal data is to be processed in this manner, such processing can only be carried out if one of the following applies:

   a) the data subject has given their explicit consent; or

   b) the processing is necessary for reasons of substantial public interest.

5. Where decisions are to be based solely on automated processing (including profiling), data subjects have the right to object, to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation of the decision from the Company. Data subjects must be explicitly informed of this right at the first point of contact.

6. In addition to the above, clear information must be provided to data subjects explaining the logic involved in the decision-making or profiling, and the significance and envisaged consequences of the decision or decisions.

7. When personal data is used for any form of automated processing, automated decision-making, or profiling, the following shall apply:

   a) appropriate mathematical or statistical procedures shall be used;

   b) technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

   c) all personal data to be processed in this manner shall be secured in order to prevent discriminatory effects arising (see Parts 25 to 30 of this Policy for more details on data security and organisational measures).**]**

23. **[Direct Marketing**

1. The Company is subject to certain rules and regulations when marketing its products **AND** services.

2. The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

   a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.

3. The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

4. If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

24. **Personal Data Collected, Held, and Processed**

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
Name	Name	Ensure correct and appropriate contact
Age	Age	Ensure contact is age appropriate and safeguards are met
Address	Address	Measure and assess geographic impact
Email	Email	Ensure correct contact method is used and to be environmentally friendly
Ethnicity	Ethnicity	For analytical purposes and to gauge impact and engagement

25. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

1. All emails containing personal data must be encrypted using encryption services provided by email provider website.com
2. All emails containing personal data must be marked "confidential";
3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
4. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
5. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
6. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
7. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a credible currier service.
8. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential";

26. **Data Security - Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
3. All personal data stored electronically should be backed up regularly with backups stored onsite **AND** offsite. All backups should be encrypted

4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise **[**without the formal written approval of Executive Directors and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

5. No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

27. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

28. **Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Executive Directors

2. No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of Executive Directors

3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

4. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

5. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Executive Directors to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS;

29. **Data Security - IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. **[**All software used by the Company is designed to require such passwords.

2. Under no circumstances should any passwords be written down or shared between

any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

3. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

4. No software may be installed on any Company-owned computer or device without the prior approval of the Executive Directors

30. **Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

2. Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

3. All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

5. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

6. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

7. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

8. All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

9. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

10. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

11. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;

12. Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

31. **Transferring Personal Data to a Country Outside the EEA**

1. The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
    1. the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
    2. the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
    3. the transfer is made with the informed and explicit consent of the relevant data subject(s);
    4. the transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
    5. the transfer is necessary for important public interest reasons;
    6. the transfer is necessary for the conduct of legal claims;
    7. the transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
    8. the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

32. **Data Breach Notification**

1. All personal data breaches must be reported immediately to the Company's Data Protection Officer.
2. If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.
3. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
4. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 32.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

5. Data breach notifications shall include the following information:
    1. The categories and approximate number of data subjects concerned;
    2. The categories and approximate number of personal data records concerned;
    3. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
    4. The likely consequences of the breach;
    5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

005 Complaints Policy

Date Created:	August 2020
Date Updated:	October 2020
Review Date:	October 2021

BVC aims to provide a safe, positive and high quality service for the BAME Community. BVC believes that the best way to ensure quality of service is to listen to the views of our staff, volunteers and partner organisations, and take these views into consideration when making changes or reviewing services. We encourage those we work with to share with us what we are doing well, but also highlight areas where we could improve. This helps us improve our service.

BVC believes that dealing with complaints is a normal and healthy part of providing our service.

What to do if you are unhappy about something at BVC

- If you are unhappy or concerned about any part of BVC's service, the first thing to do is to talk to our member of the team you know the best. This may be a Director or Non-Executive Director. It is their job to listen to your complaint and to respond to your concerns, even if the concern is about them.
- Most concerns will be dealt with quickly and easily by having a chat and putting a plan in place to make things better.
- All our team are happy to listen to your concerns.
- If you do not feel comfortable discussing your concerns with a member of the team you can request a complaints form via the website www.blackvoicescornwall.org.

What to do if you are not satisfied

- If you do not feel satisfied your concerns have been addressed you can make a complaint to a BVC Director. You can do this over the phone, by letter, or by email. It is the job of the Directors to ensure everything is working well at BVC, and to listen and respond to your concerns.
- If you feel nervous about talking on the phone or writing a letter, ask a member of the team for some help.
- The Director will usually address your concerns with you.
- On the occasion where additional information is required we will aim to respond within 14 days from the date of your initial complaint. On rare occasions this may take longer, but you will be informed of this.
- Records of your complaint and BVC's response will be stored as part of our records.

What to do if you are still not satisfied

- In order to ensure BVC works in a safe manner we have adopted the use of an Assurance Board.

- Part of the Assurance Board's job is to investigate and respond to formal complaints, in cases where the person with the complaint has not been satisfied by the response from BVC Directors.

- If you are not satisfied with the response from BVC Directors, you need to contact the Chair of The Assurance Board. BVC Directors will tell you how to go about this, and offer you help to do this.

006 Anti Racism Policy

Date Created:	**August 2020**
Date Updated:	**October 2020**
Review Date:	**October 2021**

Black Voices Cornwall will not tolerate any intentionally hostile or offensive act by a person of one racial and ethnic origin against a person of another origin, or any incitement to commit such an act in such a manner:

- That it interferes with the peace and comfort of the person
- That the quality of life of the person is reduced.

PURPOSE

- To remove any racial intolerance from Black Voices Cornwall and to promote a positive multicultural organisation.
- To allow all associates to experience a multicultural environment
- To enable all associates to thrive in a socially cohesive community.

CATEGORIES OF RACIST BEHAVIOUR

- Physical assault against a person or group because of colour and/or ethnicity
- Racist graffiti
- Provocative behaviour, e.g. racist badges or insignia
- Bringing racist materials such as leaflets/posters into the work environment inc. virtual and digital settings
- Verbal abuse and threats including name-calling, insults and racist jokes
- Incitement of others to behave in a racist way
- Racist comments in the course of discussion or correspondence
- Ridiculing of an individual or group for cultural differences
- Refusal to co-operate with others because of their ethnic origins
- Posting any racist comments onto a computer/social media platforms/ any BVC associated platforms

MONITORING AND REVIEW

Executive Directors, supported by the non-executive board, will review the policy annually.

Communications Director (Executive) will monitor anti-racist incident and records quarterly and will collate information of all incidents and then log them accordingly.

Procedures/Implementation

No associate should ignore any form of racist behaviour within the organisation (also see Equalities, Diversity and Inclusion Policy). All incidents of racist behaviour by anyone should be reported to the Communications Director, who will record it in the relevant recording system.

All incidents are recorded and followed up with the victim(s) and offenders where appropriate after four and eight weeks to ensure the racism has stopped.

Offenders should be referred to the Communications Director. The expectation is that sanctions will be applied.

Resources should:

- Reflect the fact that we are a multicultural society containing many ethnic groups
- Present positive images of people from ethnic minority groups and avoid racial stereotyping
- Present a balanced world perspective and an unbiased view of social and economic relations to the world
- Avoid tokenism either in style or content.

These resources should be regularly reviewed by Executing Directors and Non-Executive Directors.

007 Equality, Diversity & Inclusion Policy

Date Created:	August 2020
Date Updated:	October 2020
Review Date:	October 2021

Black Voices Cornwall Ltd is committed to equality, diversity and inclusion among our workforce, and eliminating unlawful discrimination.

The aim is for our workforce to be truly representative of all sections of society and our customers, and for each member to feel respected and able to give their best.

The policy's purpose is to:

- provide equality, fairness and respect for all staff.
- Adhere to the 'Equality Act 2010' and not discriminate based on any of the protected characteristics included, such as:
    - age,
    - disability,
    - gender reassignment,
    - marriage and civil partnership,
    - pregnancy, paternity or maternity,
    - race (including colour, nationality, and ethnic or national origin),
    - religion or belief,
    - sex and sexual orientation

The organisation commits to:

- Encourage equality, diversity and inclusion in the workplace.
- Create a working environment free of bullying, harassment, victimisation and discrimination, promoting dignity and respect for all, and where individual differences and the contributions of all staff are recognised and valued.
- Training managers and all other employees about their rights and responsibilities under the equality, diversity and inclusion policy. Responsibilities include staff conducting themselves to help the organisation provide equal opportunities in employment, and prevent bullying, harassment, victimisation and discrimination.
- All staff should understand that they, as well as BVC Directors, can be held liable for acts of bullying, harassment, victimisation and discrimination, in the course of their employment, against fellow employees, customers, suppliers and the public

- Take seriously complaints of bullying, harassment, victimisation and discrimination by fellow employees, customers, suppliers, visitors, the public and any others in the course of the organisation's work activities. Such acts will be dealt with as misconduct under the organisation's grievance and/or disciplinary procedures, and appropriate action will be taken. Particularly serious complaints could amount to gross misconduct and lead to dismissal.

  Further to the above, sexual harassment may amount to both an employment rights matter and a criminal matter. In addition, harassment under the 'Protection from Harassment Act 1997' is a criminal offence.

- Make opportunities for training, development and progress available to all staff, who will be helped and encouraged to develop their full potential, so their talents and resources can be fully utilised to maximise the efficiency of the organisation.

- Review practices and procedures when necessary to ensure fairness, and also update them and the policy to take account of changes in the law.

Details of the organisation's grievance and disciplinary policies and procedures can be sourced by request. This includes with whom any staff should raise a grievance.

008
Social Media Policy

Date Created:	**February 2021**
Date Updated:	**February**
Review Date:	**October 2021**

TABLE OF CONTENTS

STATEMENT AND SCOPE

As an employee and representative of Black Voices Cornwall, you are expected to demonstrate best practices and appropriate etiquette on social media, including but not limited to the following:

- Be respectful
- No hate speech
- Do not share confidential company information
- No spam
- No promotion of third party organisations without prior consent
- Be defamatory of any person
- Do not deceive others
- Do not be obscene, offensive, threatening, abusive, hateful, inflammatory or promote sexually explicit material or violence.
- Do nor promote discriminations based on race, sex, religion, nationality, disability, sexual orientation or age.
- Do not breach any of the any of the platforms own terms or guidelines.
- Do not be off topic, irrelevant or unintelligible.
- Do not advertise or promote any services without any prior agreement

Customer Inquiries

All enquiries are to be requested via email to info@blackvoicescornwall or any other appropriate point of contact at BVC.

Questionable content

Any content which might be considered questionable should be referred to Comms Director for review immediately.

TACTICAL GUIDELINES FOR EMPLOYEES

When do I need approval to post a message on social media?

All post by or on behalf of BVC should be approved by the Comms Lead.

What kind of information am I allowed to post related to my work on social media?
Any third party advertising or sharing of third part information, including your own work outside BVC should be approved by Comms Lead.

Should I include my company info in my social media bio? Or should I keep my company accounts and my personal accounts separate?
Personal and professional company informations should be kept separate at all times, unless prior approval has been granted by Comms Lead

What should I do on social media during a PR crisis?
During a PR crisis all BVC related Comms will dome directly from the Comms Lead, in exceptional circumstances the Assurance Board may intervene.

How do I comply with copyright law on social media?
If you are in any doubt of potential copyright infringements please seek advise from Comms Lead.

ANNUAL REVIEW

This policy will be reviewed once per year. All employees will be provided with access to a copy.

BLACK VOICES CORNWALL

Code of Conduct

Date written	Created by	To be reviewed	Date of any amendments
7th August 2020	Helen Hutchinson	August 2021	

As Black Voices Cornwall is an organisation that is increasing in interest and exposure it is important that everybody involved follows our code of conduct.
We desire to include everybody and their voice but in order to be effective, efficient and protect the reputation of the organisation we need everybody to agree to the following:

As a member of Black Voices Cornwall, I will:

1. Be respectful of all other members and their opinions, if it arises, to engage in healthy conversation but not to allow conversations to derail meetings
2. Maintain confidentiality – this includes not sharing any documentation outside of the group
3. Not speak in the name of Black Voices Cornwall – this is the role of directors
4. Respect the agenda of the meetings and make positive/constructive contributions
5. Work to help BVC achieve its aims and objective and not have my own agenda
6. Communicate effectively with BVC – I will send my apologies if I am not able to attend meetings or if I will be late due to circumstances
7. Promote BVC positively
8. Not bring BVC into disrespect – if for any reason I have a complaint or disagreement against BVC I will follow the correct procedures and not air my grievances publicly

BVC maintain the right to remove a member from the organisation if the above is not adhered to.

Let us all work tirelessly to achieve BVC Mission:

BVC exist to enable Cornwall to become an actively anti-racist County. We will bring increased awareness and empowerment through Communication, Education and Unification.