Data Protection Policy

Monitoring Responsibility **Board of Directors:** **Iain Woodbridge** *Iain* **Toni Matthews** *Toni* **James Matthews Woodbridge** *James* **Diana Glencross** *Diana*	Prepared by Iain Woodbridge Designated Safeguarding Lead
Next Review Date 1st September 2025	Annual Review Cycle: Unless updates and review actioned
Date Implemented 1st September 2024	
To be read with the following Policies: Cyber Security Safeguarding & Child Protection Mobile Devices & Acceptable Use Staff Code of Conduct Online Safety	Named in this Document: Iain Woodbridge Data Protection Officer and Designated Safeguarding Lead Toni Matthews Deputy Data Protection Officer Senior Leadership Team: Gemma Richards HR & Administration James Matthews Woodbridge Director & Site Lead Sheryl Dyer Support Lead, School Nurse & Duty Site Manager Tara Ballam Xtreme Director & Site Lead - Deputy Designated Safeguarding Lead

Contents:

Statement of Intent

The Ranch Xtreme aims to ensure that all personal data collected about staff, pupils, parents, directors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Providing accessible information to individuals about the use of personal data is a key element of the Data Protection Act 1998 and General Data Protection Regulation. This privacy notice explains how we collect, store and use personal data about pupils.

Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

The Definitions: Ranch Xtreme is the 'data controller' for the purposes of data protection law.

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organization that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
Provision, Site, Setting	Refers to The Ranch Xtreme as a whole.

The data controller

The Ranch processes personal data relating to parents, pupils, staff, Directors, visitors and others, and therefore is a data controller.

Roles and responsibilities

This policy applies to **all staff** employed by The Ranch, and to external organizations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The Board of Directors

The Board of Directors has overall responsibility for ensuring that The Ranch Xtreme complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to The Board of Directors and, where relevant, report to the board their advice and recommendations on the provision's data protection issues.

The DPO is also the first point of contact for individuals whose data The Ranch Xtreme processes, and for the ICO.

Our DPO is Iain Woodbridge - Designated Safeguarding Lead Level 3

The deputy DPO is Toni Matthews - Lead Inclusion Facilitator

Senior Leadership Team (SLT)

The SLT acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

Collecting, storing and processing any personal data in accordance with this policy

Informing The Ranch Xtreme of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Data protection principles

The UK GDPR is based on data protection principles that our provision must comply with. The principles say that personal data must be:

Processed lawfully, fairly and in a transparent manner

Collected for specified, explicit and legitimate purposes

Adequate, relevant and limited to what is necessary to fulfill the purposes for which it is processed

Accurate and, where necessary, kept up to date

Kept for no longer than is necessary for the purposes for which it is processed

Processed in a way that ensures it is appropriately secure

This policy sets out how The Ranch Xtreme aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

The data needs to be processed so that The Ranch Xtreme can **fulfill a contract** with the individual, or the individual has asked The Ranch Xtreme to take specific steps before entering into a contract

The data needs to be processed so that The Ranch Xtreme can **comply with a legal obligation**

The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life

The data needs to be processed so that The Ranch Xtreme as an education setting can **perform a task in the public interest or exercise its duty to Safeguard children.**

The data needs to be processed for the **legitimate interests** of The Ranch Xtreme or a third party, provided the individual's rights and freedoms are not overridden

The individual (or their parent/carer when appropriate) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defense of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research

purposes, or statistical purposes, and the processing is in the public interest

For criminal offense data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defense of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the provision's record retention schedule.

The personal data we hold

Personal data that we may collect, use, store and share (where appropriate) about pupils includes, but is not restricted to:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address) · characteristics (such as ethnicity, language)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment
- behavioral information (such as exclusions from previous settings and any relevant alternative provision put in place) · details of any support received, including care packages, plans and support
- · photographs

We may also hold data about pupils that we have received from other organizations, including other schools, local authority agents.

Why we collect and use this data

We collect and use pupil information for the following purposes:

· to support pupil learning
· to monitor and report on pupil progress
· to provide appropriate pastoral care
· to protect pupil welfare
· to assess the quality of our services

Our legal basis for using this data

We only collect and use pupils' data where the law allows us to. Most commonly, we process it where:

· we need to comply with a legal obligation

· we need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

· we have gained consent to use it in a certain way

· we need to protect the individual's vital interests (or someone else's interest)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupil's personal data overlap, and there may be several grounds which justify our use of this data.

Collecting pupil information

We collect pupil information via admission forms or secure encrypted email files from previous schools.

Pupil data is essential for The Ranch Xtreme's operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data

We keep personal information about pupils while they are attending our alternative provision. We hold this pupil data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please contact the Designated Safeguarding Lead.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- the pupil's family and representatives to provide reports, assessment information · Examining bodies ASDAN
- Ofsted
- Health authorities to keep informed with pupil's health conditions and to work with health professionals
- Health and social welfare organizations such as SWIFTS and CAMHS
- Professional advisers and consultants to advise The Ranch Xtreme on educational and complex health issues · Police forces, courts, tribunals to meet legal obligations

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

Held Information

It is held in electronic format. This information is securely protected and only accessible to nominated staff.

Parents and pupil's rights regarding personal data

Individuals have a right to make a 'subject access request' to gain access to personal information that The Ranch Xtreme holds about them.

Parents and carers can make a request to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12) or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data The Ranch Xtreme holds about them.

- If you make a subject access request, and if we do hold information about you of your child, we will: ·
- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not you or your child
- Tell you who it has been, or will be shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organization in certain circumstances.

Parents and carers also have a legal right to access to their child's educational record.

The Ranch Xtreme Workforce

We process personal data relating to those we employ to work at our provision. This is for employment purposes to assist in the running of The Ranch Xtreme and to enable individuals to be paid. The categories of information that we process include:

- personal information (such as name, address, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- Qualifications

Why we collect and use workforce information

We use workforce data to:
a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) allow better financial modeling and planning
e) enabling ethnicity and disability monitoring

Under the General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:
The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Collecting workforce information

We collect personal information via Sharepoint365 by way of secure staff contract forms and electronic forms, self completing medical and emergency information, payroll and reference details.

Whilst the majority of personal information staff provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, The Ranch Xtreme will inform the staff member at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information
We hold data securely for the set amount of time shown in our data retention schedule.

Who we share workforce information with

We routinely share this information with:
our local authority (where applicable)

Why we share workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the Education Workforce) (England) Regulations 2007 and amendments.

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

We need to liaise with other agencies – we will seek consent as necessary before doing this

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that The Ranch Xtreme holds about them. This includes:

Confirmation that their personal data is being processed

Access to a copy of the data

- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address

- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our setting may not be granted without the express permission of the pupil.

This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 academic days of receipt of a written request.

If the request is for a copy of the educational record, The Ranch Xtreme may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual.

Photographs and videos

As part of our activities, we may take photographs and record images of individuals within The Ranch Xtreme on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at The Ranch Xtreme events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where The Ranch Xtreme takes photographs and videos, uses may include:

Within setting on notice boards and ClassDojo, brochures, newsletters, etc.

Outside of The Ranch Xtreme by external agencies such as the newspapers, campaigns

Online on our website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfill their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where The Ranch Xtreme's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our provision and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

The Ranch Xtreme has a paperless administration system, hosted on the secure SharePoint365 password protected system. Paper-based records, if used at all and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use

Papers containing confidential personal data must not be left on office desks, on staff room tables, or left anywhere else where there is general access

Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

Staff, pupils or Directors who store personal information on their personal devices are expected to follow the same security procedures as for The Ranch Xtreme owned equipment

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

Electronic Folders containing personal information of pupils will be set for deletion and held in a separate archive folder until that time.

Personal data breaches

The Ranch Xtreme will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, the DPO will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in The Ranch Xtreme context may include, but are not limited to:

- Safeguarding information being made available to an unauthorized person
- The theft of a laptop containing non-encrypted personal data about pupils

Training

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Ranch Xtreme's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full Directors board.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

· object to processing of personal data that is likely to cause, or is causing, damage or distress
· prevent processing for the purpose of direct marketing

· object to decisions being taken by automated means
· in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and · a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Designated Safeguarding Lead.
Alternatively, you can make a complaint to the Information Commissioner's Office:

· Report a concern online at https://ico.org.uk/concerns/
· Call 0303 123 1113
· Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you would like to discuss anything in this privacy notice, please contact the Designated Safeguarding Lead at The Ranch Xtreme.

·Mr Iain Woodbridge

The Ranch Weymouth

Unit 21

Basepoint Business Centre

Jubilee Close

Weymouth

Dt4 7bs

Email: woody@theranchweymouth.com

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorized people

- The DPO will request that all files that contain personal information are securely closed to any and all access until the suspected breach has been investigated.
- All Staff will have passwords revoked and reassigned once the investigation has concluded.
- Staff and directors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the board of Directors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should
- take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of The Ranch's awareness of the breach. As required, the DPO will set out:
- A description of the nature of the personal data breach including, where possible:

The categories and approximate number of individuals concerned

The categories and approximate number of personal data records concerned

The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of The Ranch Xtreme's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Where The Ranch is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

• A description, in clear and plain language, of the nature of the personal data breach •

The name and contact details of the DPO

• A description of the likely consequences of the personal data breach

• A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

• Facts and cause

• Effects

• Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records and details of all breaches will be stored on The Ranch Xtreme's Safeguarding Hub on Sharepoint365 system on a secure file.

The DPO and Directors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the external IT support provider to attempt to recall it.
- In any cases where the recall is unsuccessful the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted