



DATA PROTECTION POLICY

Safeguarding Statement

At Take 2 Cornwall, we respect and value all children and are committed to providing a safe, welcoming and nurturing environment where everyone can learn and thrive. We believe every child has the right to participate fully in Take 2 Cornwall life, free from harm, neglect, abuse and discrimination.

Safeguarding and promoting the welfare of children is a legal responsibility shared by every adult working with Take 2 Cornwall Ltd. We are committed to a culture of vigilance where the best interests of the child come first, and where early help and timely intervention prevent harm from occurring.

In line with *Keeping children safe in education*, our policies and practice aim to protect children from all forms of abuse and neglect, including physical abuse, sexual abuse, emotional abuse, neglect, child-on-child abuse, exploitation, online abuse and exposure to extremist views. We work in partnership with children, parents, carers and other agencies to ensure that every child feels safe, supported and able to achieve their full potential.

This policy will be reviewed **annually**.

Overview

With provisions working with vast quantities of personal data of children and staff, data protection is vital.

The Data Protection Act (DPA) was updated to the GDPR in May 2018, changing regulations throughout Europe around data protection. GDPR classifies the data that provisions handle as 'special category data'. This form of data is subjected to tight controls, which means provisions must adhere to GDPR guidelines and efficiently protect this information.



Data protection is safeguarding private and important information from compromise, corruption, and loss.

Take 2 Cornwall will ensure that we act per UK data protection law by collecting, storing and processing all personal data collected about all stakeholders, including staff, children, parents, governors and visitors, in line with this legalisation.

This policy applies to the handling of all personal data, be it on paper or in an electronic format.

Legislation and guidance

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and meets the requirements of the:

- [Data Protection Act 2018 \(DPA 2018\)](#)
- [The Data Protection, Privacy and Electronic Communications \(Amendments etc.\) \(EU Exit\) Regulations 2020](#)

Definitions and Terms

Data controller

The individual or organisation that has the responsibility for data protection regulation compliance and managing how data is processed.

Data processor

The individual or other body processing identifiable personal data. They do this on behalf of the data controller.

Data subject

The identifiable individual whose personal data is held or being processed.

Personal data

The information of a living individual which can identify them, i.e. name (including initials), identification number/s, location data or online identifier (i.e. a username), medical, economic, cultural, physical or genetic identity.

Personal data breach

A breach of security which leads to accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data.



Processing

When anything is done to personal data manually or electronically, collecting, recording, organising, structuring, storing, adapting, changing, altering, retrieving, using, disseminating, erasing or destroying.

Special categories of personal data

Special categories which require the most protection as it is of a more sensitive and personal nature; race, political views, religious belief, medical/health information, sexual orientation, genetic information, biometric information, membership of specific groups such as trade unions

The data controller

Take 2 Cornwall is a data controller as it processes personal data which pertains to children, staff, parents, visitors and other persons such as contractors.

Take 2 Cornwall, as is legally required, is registered with the ICO / has paid its data protection fee to the ICO. Take 2 Cornwall registration reference is: ZA509436

Roles and responsibilities

All staff employed by Take 2 must adhere to this policy. Non-compliance with the policy by staff may result in disciplinary action being taken.

All staff

The responsibilities of the staff are to:

- Ensure they keep Take 2 Cornwall up to date on any changes to their personal data
- Ensure they act per this policy when they collect, store and process any personal data
- Ensure they make contact with the DPO in the case of the following:
 1. If they are concerned that this policy is not being followed correctly
 2. If they have worries about the legal aspect of how they are processing personal data
 3. If they have any questions concerning data protection law, retention of personal data, security of personal data or the operation of this policy
 4. If there is a data breach

5. If they are undergoing a new activity, it may affect individuals' rights of privacy
6. If they need help with the sharing of personal data or contracts with any third parties
7. If they need help to deal with the data protection rights of an individual who has invoked them, the drafting of a privacy notice or the transference of personal data outside of the UK

Data protection principles

Take 2 must comply with the UK GDPR data protection principles. These principles, as stated by the ICO ([The principles | ICO](#)), say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
- 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 ('purpose limitation')
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals ('storage limitation')
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and



accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Personal data collection

Lawfulness, fairness and transparency

The processing of **personal data** will only be undertaken if it meets the requirements of data protection law's six legal reasons or 'lawful bases'. These are the processing of data:

- To **fulfil a contract** with an individual or when an individual has requested that Take 2 takes particular steps before a contract can be entered into
- To **comply with a legal obligation** Take 2 has
- To ensure the **vital interests** of the individual or another person, such as to protect someone's life
- So that Take 2 can **perform a task in the public interest or exercise its official authority**
- In Take 2 Cornwall's **legitimate interests** (when not acting as a public authority) or a third party, provided the individual's rights and freedoms are not disregarded.
- When clear **consent** is freely given by an individual (or, in the case of a child, their parent/carer)

In the case of **special categories of personal data**, special category conditions for processing under data protection law will be met. These are the processing of data:

- When **explicit consent** is given by the individual (or, in the case of a child, their parent/carer)
- To exercise rights concerning **employment, social security or social protection law**
- To ensure the **vital interests** of the individual or another person, if they are incapable physically or legally of giving consent
- Where data has been made **manifestly public** by the individual previously
- For **legal claims** that have been established, exercised or are being defended
- For reasons, as defined in legislation, of **substantial public interest**



- For **health or social care purposes**, and when it is confidentially processed by or under the direction of a social worker or health professional or any such other person who is obliged to by law
- For **public health reasons**, and when it is confidentially processed by or under the direction of a health professional or any such other person who is obliged to by law
- For **archiving purposes**, statistical, scientific or historical research purposes and is in the public interest

Any processing under data protection law will be met for criminal offence data. These are the processing of data:

- When clear **consent** is freely given by an individual (or, in the case of a child, their parent/carer)
- To ensure the **vital interests** of the individual or another person, if they are incapable physically or legally of giving consent
- Where data has been made **manifestly public** by the individual previously
- For or in connection with legal proceedings, for the obtaining of legal advice, or for **legal rights** that have been established, exercised or are being defended
- For reasons, as defined in legislation, of **substantial public interest**

Before the first collection of personal data, individuals will be provided with the relevant information as required by data protection law.

We ensure that personal data is processed fairly, handled expectedly and used in ways which would not have an unjustified adverse effect on any individual.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons, which are explained to individuals upon their first collection.

If Take 2 Cornwall wants or needs to use personal data for any other reasons than those first given, we will inform the individuals concerned and seek consent before use.

Staff will only process personal data when it is necessary to fulfil their job role.

Take 2 Cornwall will ensure that stored data is accurate and up to date. Any inaccurate data will be amended or deleted as appropriate. Any personal data no longer required will be deleted or anonymised.



Personal data sharing

Personal data will not be shared with anyone else without consent unless, under specific certain circumstances when Take 2 Cornwall are required to do so. Such circumstances are but are not limited to, where:

- There is a risk to the **safety of our staff** through an issue with a child or parent/carer
- Other agencies require such data. Consent to share will always be sought in this case
- Take 2 Cornwall's suppliers or contractors need data to provide services to staff and children, e.g. Management Information (MIS) system or IT services. Take 2 Cornwall will therefore ensure the following:
 - o The appointment of suppliers or contractors that provide sufficient guarantees of their compliance with UK data protection law
 - o Any contract with a supplier or contractor will process personal data that Take 2 Cornwall shares fairly and lawfully
 - o Only personal data needed to carry out the service of the supplier or contractor will be shared with them.

We will share personal data when legally required to do so with law enforcement and government bodies. Similarly, Take 2 Cornwall may share personal data with emergency services and local authorities in the event of the need to respond to an emergency that affects any children or staff.

Where necessary, Take 2 Cornwall will transfer personal data internationally per UK data protection law.

Subject access requests and individual's rights

Subject access requests

To gain access to any personal information held by Take 2 Cornwall an Individual has the right to make a 'subject access request'. This request includes the following:

- Confirmation of processing of their personal data
- A copy of the data held
- Why has the data been processed
- The categories of personal data concerned; the reasons and purpose.



- With whom the data has been, or will be, shared with
- The length of time the data has been or will be stored for and, in the case of unknown time stored, the criteria used to determine this period of storage
- The right to request records are rectified, erased or restricted, or to object to such processing, where necessary
- The right to submit a complaint to the ICO or any other supervisory authority
- Where the data was sourced from, if not from the individual
- If any automated decision-making is being applied to their data, and the significance and consequences this might have for the individual
- What safeguards are in place if the data is being internationally transferred

Whilst subject access requests can be submitted in any form, requests will be processed more quickly if made in writing and include the following:

- Individual's name
- Address to receive correspondence
- Contact details- phone number and email address
- Requested information details

Any receipt of a subject access request, in any form, must be immediately forwarded to the DPO.

Children and subject access requests

The personal data of a child belongs to them, not their parents or carers. Therefore, any parent or carer making a subject access request concerning their child must have their child's consent or prove that the child cannot understand their rights and the implications of a subject access request.

The age of maturity in a child to understand their rights is deemed to be over the age of twelve. Therefore, Take 2 Cornwall will grant subject access requests from parents or carers of children without the express permission of the child where the child is below this age. However, it is important to note that this age is not a rule, so Take 2 Cornwall will judge each child's ability to understand their rights on a case-by-case basis.

Responding to subject access requests

Take 2 Cornwall will respond to requests by:

- Asking the requester to provide two forms of identification



- Confirming the request by contacting the requester by phone if possible
- Responding promptly, at least within one month of receipt of the request, where the identity has been confirmed
- Providing all information free of charge
- Informing the requester that we will comply within three months of receipt of the request in the case of complex or numerous requests. Any such need for an extension will be communicated to the requester within one month with the reasons for any such extension

For a variety of reasons, Take 2 Cornwall may not disclose information.

Such reasons include if:

- Serious harm could be caused either physically or mentally to a child or another individual
- Disclosure of the information would reveal historical or current abuse of a child, or pose a risk of abuse or where the disclosure of that information would not be in the child's best interests
- Another person's personal data would be included for which consent is not given, and the data cannot be reasonably anonymised to remove such details
- Part of the data contains sensitive documents, e.g. related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

Where requests are excessive or have an unfounded basis, Take 2 Cornwall may refuse to act upon it or reserve the right to levy a reasonable charge for administration costs. Any request of a repetitive nature will also be taken into account when making this decision.

In the case of a refusal, the requester will be told the reasons for refusal and their rights to make a complaint to the ICO or to enforce their subject access right through court proceedings.

Individual data protection rights

Individuals also have rights in addition to making a subject access request.

These rights are:

- Withdrawal of their consent to the processing of their data



- Object to the processing of their data that is used and shared based on public interest, official authority or legitimate interests
- Instruct Take 2 Cornwall to rectify, erase or restrict any processing of their personal data
- Prevent the use of their personal data for direct marketing
- Challenge decisions that have been made solely by automated decision-making or profiling (i.e. making decisions or evaluations made with no human involvement)
- Be informed of a data breach (in certain circumstances)
- Submit a complaint to the ICO
- Request their personal data be transferred to a third party in a structured, commonly used, machine-readable format

Any requests to exercise these rights should be sent to the DPO. The request must be immediately forwarded to the DPO if any other staff receives them.

Requests to see the educational records by parents

All individuals with parental responsibility have the legal right to freely access their child's educational record when a child is under 18. The request must be in writing and be responded to within 15 school days of receipt.

This right can be refused in some circumstances. Such circumstances are if releasing the requested information might cause serious harm physically or mentally to a child or another individual or if it would mean releasing exam marks before the official announcement.

Videos and photographs

Photographs and videos taken and used for communication, promotion and marketing purposes will only be used where written consent from parents/carers has been sought and Take 2 Cornwall has clearly explained how these images will be used.

Where parents/carers take photographs and videos of their child at Take 2 Cornwall events, these are for personal use and are not covered by data protection legislation. However, Take 2 Cornwall requests that parents do not photograph or video any child other than their own and not share them publicly on social media for safeguarding reasons unless all relevant parents/carers agree.



When Take 2 Cornwall takes photographs and videos, these may be used for:

- On notice boards or brochures, newsletters, etc.
- External agencies such as the school photographer, newspapers, campaigns
- Online on our website or social media pages

Consent can be refused or withdrawn at any time. The photograph or video will be deleted if consent is withdrawn and not used further.

All photographs and videos will not be accompanied by any personal information and faces and identifying features anonymised so as not to identify a CHILD.

Design and default of data protection

To ensure that Take 2 Cornwall has integrated data protection in all data processing activities, we will have the following measures in place:

- Appointment of a suitably qualified DPO with the necessary resources to maintain their expert knowledge and fulfil their duties
- In line with the data protection principles set out in relevant data protection law (see section 6), only processing personal data that is necessary for each specific purpose of processing
- As advised by the DPO, complete data protection impact assessments where our processing of personal data could pose a high risk to the rights and freedoms of individuals, as well as during the introduction of new technologies
- Ensuring that data protection is integrated into internal documents, including this policy, other related policies and privacy notices
- Ensuring staff members receive regular training on data protection law, this policy, related policies, and other data protection matters. A record of attendance will be maintained
- Testing our privacy measures and ensuring compliance by regularly conducting reviews and audits
- Ensuring that the transfer of personal data out of the UK has appropriate safeguards in place, especially where different data protection laws may apply
- Ensuring records of our processing activities are well maintained, including:



- o Make available the name and contact details of Take 2 Cornwall and DPO and all information that we are required to share about how personal data is used and processed (via privacy notices)
- o Maintain an internal record of the type of personal data held, type of data, how and why this data is used, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we keep the data secure

Data security and storage of records

Take 2 Cornwall will keep data safe and protect it from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

We will ensure the following:

- Any portable electronic devices that contain personal data (laptops, tablets, hard drives) as well as any paper-based records and are kept locked away when not in use
- Any documents containing confidential personal data will not be left out and unattended on office and classroom desks, staffroom tables or any place with general access.
- If any information which contains personal data needs to be taken off-site, then staff must sign it in and out from our office.
- Encryption software protects all portable devices and removable media, such as laptops, hard drives and USB devices.
- Any personal data information from Take 2 Cornwall stored by staff and/or children on their personal devices must follow the same security procedures as for Take 2 Cornwall owned equipment.
- In the event of sharing personal data with a third party, we will carry out due diligence, taking all reasonable steps to ensure it is stored securely and adequately protected (see [Sharing personal data](#))

Disposal of records

Take 2 Cornwall will ensure that any personal data that is no longer needed will be disposed of securely. Likewise, personal data that is inaccurate or out of date will also be disposed of securely if it cannot be rectified or updated.



We will confidentially shred or incinerate paper-based records and overwrite or delete electronic files. Take 2 Cornwall may use a third party to safely and confidentially dispose of records on our behalf. In this case, we will ensure the third party provides sufficient guarantees that it complies with data protection law.

Personal data breaches

Take 2 Cornwall will make all reasonable efforts to ensure no personal data breaches.

If appropriate, Take 2 Cornwall will report the data breach to the ICO within 72 hours of awareness. Breaches may include, but are not limited to:

- Publication of a dataset on our website which has not been anonymised
- An unauthorised person being given safeguarding information
- Non-encrypted personal data about children on a stolen company laptop
- Personal data sheet being in possession of another individual other than who it pertains to

Training

Data protection training is provided for all staff and governors during their induction process.

This policy was adopted by: Take 2 Cornwall	Date:01.09.2021
Reviewed: 01.09.2022	Signed: PJA
Reviewed: 01.09.2023	Signed: PJA
Reviewed: 30.07.2024	Signed: PJA
Reviewed: 30.07.2025	Signed: PJA
Reviewed: 01.09.26	Signed: PJA



To be reviewed: 01.09.27	Signed:
--------------------------	---------

Appendices

- 1: Data Protection Registration Certificate
- 2: Consent form for sharing information
- 3: Personal Data Audit 4: Cyber Insurance

Data Protection Registration Certificate

Take 2 Cornwall Limited

Metherell Gard
Burn View
Bude
Cornwall, EX23 8BX

Registration reference: ZA509436
Date registered: 10 June 2019
Registration expires: 09 June 2026



Issued by: Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow, Cheshire
SK9 5AF

Telephone: 0303 123 1113
Website: ico.org.uk

2: Consent form for sharing information



Consent to share information

To be signed by the person with parental responsibility

This form contains your consent to the sharing of information. The consent applies to the young person named below and where necessary may include information about the young person's health, welfare and development and their home or family circumstances.

Once permission is granted, information will be shared with relevant organisations, to assist the effective provision of family support, education or health services of the young person named below. This consent will remain valid for the time the young person is at Take 2 Cornwall and if needed in the future. It applies to information already held on file and to information subsequently added.

I agree to the personal information of the individual named below being shared for the purpose of providing services to promote welfare and meet their identified needs.	
Name: (Print)	Signed:
Date of Signature:	
Name of child:	Date of Birth:
I am satisfied that the person can understand the information that has been given to them.	
Name: (Print) Paula Atkinson	Signed: 



3: Personal Data Audit

Personal data relating to child						
Information	Format	Where information is kept	How is it kept secure	Shared with?	externally	Retained until
Medical Form	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive	Medical professionals for treatment		3 years after child leaves setting
Registration Documents	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive			3 years after child leaves setting
Referral Paperwork	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive			3 years after child leaves setting
Provision Plan	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive			3 years after child leaves setting
Allergy Information	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive			3 years after child leaves setting



Permission forms: Activities, sunscreen, photographs, skatepark, Horse Care	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive		3 years after child leaves setting
Document checklist	Electronic on Take 2 Drive	Within the Admin Team Drive	Password protected; stored using secure data service. 2-step verification		When child leaves setting

			Only Take 2 admin staff have accesses to the Take 2 admin Drive		
Incident/Accident log	Electronic on Take 2 Drive Electronic on Take 2 SharePoint	Within individual student files on the Drive Incident Log in SharePoint	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive Only senior management have accesses to the SharePoint	Educational setting, Social worker and Provision Referral originally came from	3 years after child leaves setting
Daily Session Reports	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive	Educational setting, Social worker and Provision Referral originally came from Parents if requested and they have egress	3 years after child leaves setting
Record of medication given	Paper	Child records	Locked filing cabinet	Medical professionals for emergency treatment	3 years after child leaves setting
Photographs of child	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive	Parents, carers and School	Child leaves setting

Personal data relating to parent / carer

Information	Format	Where information is kept	How is it kept secure	Shared externally with?	Retained until
-------------	--------	---------------------------	-----------------------	----------------------------	----------------



Registration Documents	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive		3 years after child leaves setting
Complaints	Email	Within the Admin Team Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 admin staff have accesses to the Take 2 admin Drive		3 years after date of complaint
General correspondence	Phone calls, Email and Text message	Take 2 Cornwall admin email account; Take 2 Cornwall phone	Email is password protected; Take 2 Cornwall phone is passcode locked		When child leaves the setting

Payment records	Electronic	Finance Managers Drive	Computer is password protected 2-step verification	Finance Manager and Metherell Guard	6 years
Emergency contact details	Electronic on Take 2 Drive	Within individual student files on the Drive On staff contacts list on mobile phone	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive		
All information in Student file	Electronic on Take 2 Drive	Within individual student files on the Drive	Password protected; stored using secure data service. 2-step verification Only Take 2 staff can sign into the Take 2 Drive	Schools. Lea and other relevant professionals	3 years after student has left unless legally required for longer

Personal data relating to staff

Information	Format	Where information is kept	How is it kept secure	Shared with? externally	Retained until
-------------	--------	---------------------------	-----------------------	-------------------------	----------------



Terms and conditions of employment	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR File	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive	External HR service	6 years from end of employment
Medical form	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR File	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment
DBS record	Scanned copies on Take 2 Drive	DBS Certificate number held on staff central record	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive	Educational settings if requested	6 years
Payroll records	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR File	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have	Payroll service	6 years

			accesses to the Take 2 HR Drive		
Training records	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive Take 2 Training drive SSS Learning Admin log-in	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment



Qualification certificates	Scanned copies on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive Training Google Drive SSS Learning Admin log -in	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive	Educational settings if requested	6 years from end of employment
Staff Reviews	Electronic on Staff Reviews Drive	Senior Management and with the manager carrying out review and staff under review. They are done monthly for the first 6 months of employment then every 6 months.	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have access to this information.		6 years from end of employment
Application form	Scanned copies or electronically on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment; unsuccessful candidates who were interviewed: 3 months; other unsuccessful candidates: disposed of immediately
Interview record	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment; unsuccessful candidates: 3 months
Timesheet	Electronic on Take 2 Drive	Excel spreadsheet within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment



References	Scanned copies or electronically on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment
Proof all Policies have been read	Electronically	SSS Learning Portal Said staff have access to their own portal	Password protected; stored using secure data service. 2-step verification Training co-ordinator and Senior Management have access to the SSS Learning Admin Portal		6 years from end of employment
Induction checklist	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		6 years from end of employment
Grievances, written warnings	Electronic on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive	External HR service	6 years from end of employment
Any other correspondence	Scanned copies or electronically on Take 2 Drive	Within individual staff HR files on the Drive. Said staff have access to their own HR drive	Password protected; stored using secure data service. 2-step verification Only Take 2 Senior Management have accesses to the Take 2 HR Drive		Staff member leaves depending on the correspondence

We also have SharePoint where information is stored only management has access to.

4: Cyber Insurance



Cyber & Technology E&O Insurance

Summary of Cover

Company: The insurance provided is through any of the following underwriting carriers: Allianz Global Corporate & Specialty SE, part of Allianz Group, Navigators Insurance, and/or Certain Underwriters at Lloyd's of London.

- Allianz Global Corporate & Specialty SE, is a part of the Allianz Group, and is a German authorised insurance company, providing insurance products and services on a cross-border basis. Allianz Global Corporate & Specialty is the UK branch of Allianz Global Corporate & Specialty SE, Königinstrasse 28, 80802 München, Germany. Munich Commercial Register HRB 208312. UK Branch Registered Office: Allianz House, 60 Gracechurch Street, London EC3V 0HR. Registered in England at UK Companies House FC039211 and BR024312. UK Financial Conduct Authority Register 214374. Authorised by Bundesanstalt für Finanzdienstleistungsaufsicht.
- Navigators Insurance Company UK Branch (trading as 'The Hartford') is registered in England and Wales under company number: BR004168. Registered office: Floors 8, 6 Bevis Marks, Bury Court, London EC3A 7BA. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. FRN: 202980.

This insurance is arranged by Coalition Risk Solutions Ltd, who have been authorised by the insurers under a delegated authority to transact insurance business and handle claims on their behalf. Coalition is a trading name of Coalition Risk Solutions Ltd, which is an appointed representative of Davies MGA Services Limited, a company authorised and regulated by the Financial Conduct Authority under firm reference number 597301 to carry on insurance distribution activities. Coalition Risk Solutions Ltd. is registered in England and Wales company number 13036309. Registered office at 34-36 Lime Street, London, United Kingdom, EC3M 7AT.

Product: Cyber and Technology Errors & Omissions Insurance

This document provides a summary of the cover, exclusions and restrictions. It is not personalised to your individual selections. The full terms and conditions of this insurance, including the general policy limits, can be found in the policy document which is available on request from your broker.

What is this type of insurance?

This is a Cyber and Technology Errors & Omissions insurance policy. Cyber insurance **covers certain losses relating to damage to, or loss of information from, IT systems and networks**. Policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement. Cover will only be provided for the sections you select, up to the agreed sum insured for each sublimit.

Cybersecurity tools and support

- Detailed, personalised cyber risk assessments
- Policyholder and pre-bind access to Coalition Control, our cybersecurity platform
- In-house cybersecurity expertise available to all policyholders
- Cyber threat updates and advice from Security Labs, our R&D team

Expert claims and incident response

- Our in-house claims team handles your cyber incident seamlessly and works with your team towards the best possible outcome
- Access to Coalition Incident Response (CIR) via panel selection means a crucial fast response when a cyber incident happens