



Data Protection and Data Security Policy

Contents

Data Protection and Data Security Policy	1
1. Statement of policy and purpose of Policy	1
2. Who is responsible for data protection and data security?	2
3. What personal information and activities are covered by this policy?	2
4. What personal information do we process about you and what do we do with it? ..	2
5. What personal information do we process about Directors/Trustees and what do we do with it?	5
6. What personal information do we process about Staff and what do we do with it? ..	6
7. Data Protection Principles.	8
8. Data security	9
9. Subject access requests	11
Annex A to OCOSC Data Protection and Data Security Policy	12
Annex B to OCOSC Data Protection and Data Security Policy	20
Annex C to OCOSC Data Protection and Data Security Policy	27

1. Statement of policy and purpose of Policy

- a. Oldbury Court Out of School Clubs (OCOSC) is committed to ensuring that all personal information handled by us will be processed accordingly to legally compliant standards of the General Data Protection Regulation (GDPR)
- b. The purpose of this policy is to help us achieve our data protection and data security aims by:
 - i. Notifying our staff and members of the types of personal information that we may hold about them and what we do with that information;
 - ii. Ensuring staff understand our rules and the legal standards for handling personal information relating to staff and club members and the children who attend our sessions
 - iii. Clarifying the responsibilities and duties of staff in respect of data protection and data security.
 - iv. Inform OCOSC members of our obligations under the regulations and the rights club members have under the GDPR Regulations.
- c. This is a statement of policy only and does not form part of your contract of employment and/or club membership. We may amend this policy at any time, in our absolute discretion.



- d. Notification of amendments shall be published via our Newsletter and our Facebook site. The Amended policy shall be posted on our Website Policy Page and a hard copy retained in our policy file held in the OCOSC main site office, Christ Church Out of School Club and Chester Park After School club.

2. Who is responsible for data protection and data security?

- a. Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors, trustees and officers, consultants, contractors, casual or agency staff, trainees, homeworkers, fixed-term staff and any volunteers.
- b. The board of directors of the OCOSC has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed the OCOSC Manager as the Data Protection Officer with day-to-day responsibility for data processing and data security.
- c. All Staff, Directors and trustees have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance.
- d. Any breach of this policy will be taken seriously and may result in disciplinary action.

3. What personal information and activities are covered by this policy?

- a. This policy covers personal information:
 - i. which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess;
 - ii. is stored electronically or on paper in a filing system;
 - iii. in the form of statements of opinion as well as facts;
 - iv. which relates to Staff (present, past or future);
 - v. Club Members (present, past or future);
 - vi. Children who use our services (present, past or future);
 - vii. Individuals listed as Emergency Contact (present, past or future);
 - viii. any other individual whose personal information we handle or control;
 - ix. Which we obtain, hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

4. What personal information do we process about you and what do we do with it?

- a. We collect personal information about you which:
- b. You provide or we gather before or during your membership with us;
- c. Falls within one or more of the six lawful bases for processing data as set out in Article 6 of the GDPR. See Annex A for more detail.



d. The types of personal information that we may collect, store and use about you include records relating to your:

- i. Names of your children, age and date of birth
- ii. Nationality
- iii. Your and if relevant Partners details
 - a. Full address
 - b. Home telephone number
 - c. Mobile telephone number
 - d. Email address
 - e. Occupation
 - f. National Insurance number
 - g. Name of employer
 - h. Work telephone number
 - i. Which parent/carer the child(ren) normally lives with.
- iv. Emergency Contact name, telephone and mobile numbers
- v. Names of persons authorised to collect the children.
- vi. Medical details
 - a. Name of doctor
 - b. Doctors telephone number
 - c. Doctors Address
 - d. Details of Children's special needs/disabilities/allergies where applicable

e. We record if you have provided; -

- i. Permission for your children to appear in photographs used for publicity
- ii. Permission for your children to appear in any image displayed on our website
- iii. Permission for your children names to be used in articles relating to OCOSC on our website
- iv. Permission to use your email address to send information relating to our services to you.
- v. Permission for your child to apply sun cream in hot conditions
- vi. Accepted responsibility to ensure your children have suntan protection before attending club.
- vii. Permission for OCOSC to take your children to school, collect from school and take part in planned trips and local outings accompanied by OCOSC staff.
- viii. Authorisation for the play leader to sign any documents required by the hospital authorities if and only if either parent/guardian or emergency contacts can be reached by phone or other means to authorise emergency medical/dental treatment.
- ix. Details of any other adult who may have a legal right to contact and/or have parental responsibility for any of your children not listed on your membership registration form. These details are collected by you with their consent and supplied to us on a separate Registration form.
- x. Any other relevant information provided by you on the annual registration form.



NOTE as club member, it is your responsibility, to ensure that the details you provide to us correct and up to date, that details provided by you concerning your partner, emergency contacts and persons nominated to collect your children are provided to use with their permission. That you ensure that they are made aware of our policy and that it is available for them to download from our website policy page.

- f. We will use information to carry out our business, to administer your membership and the services we provide to you including:
- i. Evacuation List: to compile and circulate lists of home address and contact details, to contact you outside working hours.
 - ii. Medical records
 - iii. Minibus emergency contact folder
 - iv. Disciplinary, grievance or legal matters: in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.
 - v. Registration folders.
 - vi. Signing In/out sheets
 - vii. Tuck shop book records money held on member's behalf for the purpose of enabling your child to buy tuck.
 - viii. Funding folder for 1:1 support applications
 - ix. Letters folder- retention of any letters sent or received to/from club members in relation to our services
 - x. Confidential File- if involved in a disclosure Incident as required by Bristol councils safeguarding policy.
 - xi. Bristol Standards folder – photos in support of our award.
 - xii. Directors File- information required by Charity commission/company House/Ofsted
 - xiii. Equal Opportunities monitoring: to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of our membership required as evidence in support of grant/fundraising applications.
 - xiv. Adult and child incident folder – record and statements of any incidents
 - xv. Vulnerable Persons protection folder
 - xvi. Support workers folder
 - xvii. Individual Behaviour management plans
 - xviii. Voucher Company records
 - xix. Student folder – documentation in support of adult student support applications
 - xx. Lost deposit folder
 - xxi. Invoices
 - xxii. Receipts
 - xxiii. Bank Statements
 - xxiv. Register
- g. We confirm that for the purposes of the Data Protection Act 1998 and under the GDPR, OCOSC is a Data Controller of the personal information in connection with your membership. This means that we determine the purposes for which, and the



manner in which, your personal information is processed.

- h. If you consider that any information held about you is inaccurate then you should notify the OCOSC manager or the Data Protection Officer by means of a formal letter and, if we agree that the information is inaccurate then we will correct it. If we do not agree with the correction then we will note your comments.
- i. We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside OCOSC. However, we may need to disclose personal information about you/your children:
 - i. for the administration of your membership account and associated benefits eg Student loans,
 - ii. to comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation use of the services OCOSC provide to you, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities, such as HM Revenue and Customs, Ofsted, Social Services ect.
 - iii. to other parties such as the schools your children attend.
- j. In all instances disclosure of personal information about you or your children shall only occur where OCOSC can clearly demonstrate that such a disclosure is permissible under the lawful bases for processing as set out in article 6 of the GDPR
- k. By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

5. What personal information do we process about Directors/Trustees and what do we do with it?

- a. In addition to the information we collect as a member of the club OCOSC also collect and retain the following:
 - i. Disclosure and Barring Service reference number
 - ii. Training records
 - iii. Photographs
 - iv. Date of Birth
 - v. Address
 - vi. Nationality.
- b. We will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns including:
 - i. OCOSC management Lists: to compile and circulate lists contact details, to contact you
 - ii. Monitoring IT systems: to monitor your use of OCOSC e-mails, internet, telephone, computer or other communications or IT resources.
 - iii. Disciplinary, grievance or legal matters: in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may



- involve you.
 - iv. Publicity of directors and trustee to the club membership on notice boards
 - v. Equal Opportunities Monitoring: to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of the Employer's workforce.
- c. We confirm that for the purposes of the Data Protection Act 1998 and under the GDPR, the OCOSC is a Data Controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal information is processed.
- d. If you consider that any information held about you is inaccurate then you should tell Chair of the management committee and or the Data Protection Officer and, if we agree that the information is inaccurate then we will correct it. If we do not agree with the correction then we will note your comments.
- e. We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside the Employer. However, we may need to disclose personal information about directors and trustees for the administration of club
- f. to comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to Charity governance, management and administration, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities, such as Company House, The charity commission, Ofsted , Social Services ect.
- g. to other parties such as the schools OCOSC provide a collection service.
- h. In all instances disclosure of personal information about directors and trustees shall only occur where OCOSC can clearly demonstrate that such a disclosure is permissible under the lawful bases for processing as set out in article 6 of the GDPR
- i. By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

6. What personal information do we process about Staff and what do we do with it?

- a. We collect personal information about you which:
- i. you provide or we gather before or during your employment or engagement with us;
 - ii. is provided by third parties, such as references or information from suppliers or another party that we do business with; or
 - iii. is in the public domain.
 - iv. Falls within one or more of the six lawful bases for processing data as set out in Article 6 of the GDPR. See Annex A for more detail.
- b. The types of personal information that we may collect, store and use about you include records relating to your:



- i. Home address and contact details as well as contact details for your next of kin;
 - ii. Recruitment (including your application form or cv, any references received and details of your qualifications);
 - iii. Pay records, national insurance number and details of your taxes and any employment benefits such as pension and health insurance (including details of any claims made);
 - iv. Any sickness absence or medical information provided;
 - v. Religious or philosophical beliefs (eg specific dietary or holiday requirements);
 - vi. Information about your race, colour, nationality, or ethnic or national origins;
 - vii. Sexual orientation, where this is disclosed to us (eg through providing details of your spouse or partner for the administration of benefits);
 - viii. Telephone, email, internet, fax or instant messenger use;
 - ix. Performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.
 - x. Photographs
 - xi. Next of Kin details, where this is disclosed to us.
 - xii. Details of passport/Id documents proving eligibility to work in the UK
 - xiii. Driving Licence details.
- c. We will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have including:
- i. **Staff Address Lists:** to compile and circulate lists of home address and contact details, to contact you outside working hours.
 - ii. **Sickness records:** to maintain a record of your sickness absence and copies of any doctor's notes or other documents supplied to us in connection with your health, to inform your colleagues and others of that you are absent through sickness, as reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.
 - iii. **Monitoring IT systems:** to monitor your use of OCOSC e-mails, internet, telephone, computer or other communications or IT resources.
 - iv. **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.
 - v. **Performance Reviews:** to carry out performance reviews.
 - vi. **Notice boards photos** to enable children and club members to recognise you as a member of staff. Nominated first aiders and other associated H&S responsibilities.
 - vii. **Equal Opportunities Monitoring:** to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of the Employer's workforce.
- d. We confirm that that for the purposes of the Data Protection Act 1998 and under the GDPR, the Employer is a Data Controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the



manner in which, your personal information is processed.

- e. If you consider that any information held about you is inaccurate then you should tell your line manager or the Data Protection Officer and, if we agree that the information is inaccurate then we will correct it. If we do not agree with the correction then we will note your comments.
- f. We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside the Employer. However, we may need to disclose personal information about Staff:
 - i. for the administration of your employment and associated benefits e.g. to the providers of our pension or insurance schemes; or
 - ii. to comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to employment issues, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities, such as HM Revenue and Customs, Ofsted, Social Services etc.
 - iii. to other parties such as the schools OCOSC provide a collection service.
- g. In all instances disclosure of personal information about staff shall only occur where OCOSC can clearly demonstrate that such a disclosure is permissible under the lawful bases for processing as set out in article 6 of the GDPR
- h. By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

7. Data Protection Principles.

- a. Staff whose work involves using personal data relating to Staff, Directors, Trustees, Club members, next of Kin, Emergency Contacts, children using the service or others must comply with this policy and with the eight legal data protection principles which require that personal information is:
 - i. **Processed fairly and lawfully.** We must always have a lawful basis to process personal information. In most (but not all) cases, the person to whom the information relates (the Subject) must have given consent. The Subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.
 - ii. **Processed for limited purposes and in an appropriate way.** Personal information must not be collected for one purpose and then used for another. If we want to change the way we use personal information we must first tell the Subject.
 - iii. **Adequate,** relevant and not excessive for the purpose.
 - iv. **Accurate.** Regular checks must be made to correct or destroy inaccurate information.
 - v. **Not kept longer than necessary for the purpose.** Information must be destroyed or deleted when we no longer need it. For guidance on how long particular information should be kept, contact the Data Protection Officer.



- vi. **Processed in line with Subjects' rights.** Subjects have a right to request access to their personal information, prevent their personal information being used for direct-marketing, request the correction of inaccurate data and to prevent their personal information being used in a way likely to cause them or another person damage or distress.
- vii. **Secure.** See further information about data security below.
- viii. **Not transferred** to people or organisations without adequate protection.
- ix. **Not transferred** to people or organisations situated in other countries without adequate protection.

b. Personal Information **may not be passed third parties without**

- i. The individual/organisation receiving the information having first provided OCOSC a copy of their current Data Protection Policy.
 - ii. Confirming that there is a justifiable and legal requirement for the information to be passed to the third party.
 - iii. The individual/organisation receiving the information provides written confirmation that the data will not be passed onto other organisations without written permission from OCOSC/individual concerned, That the information is only used for the reason for which it was obtained and retained for as long as is legally permitted, afterwards they shall dispose of the data in accordance with this policy.
 - iv. OCOSC shall retain a copy of the third party's data protection policy, the written confirmation detailed in par 18.j.iii above, together with details as to what type of data was provided (not the individuals data), to whom, why it was required and for how long that organisation intends to hold onto the data. This information shall be kept on file for 5 years.
- c. Some personal information needs even more careful handling. This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about criminal offences. Strict conditions apply to processing this sensitive personal information and the Subject must normally have given specific and express consent to each way in which the information is used.

8. Data security

- a. We must all protect personal information in our possession from being accessed, lost, deleted or damaged unlawfully or without proper authorisation through the use of data security measures.
- b. Maintaining data security means making sure that:
 - i. only people who are authorised to use the information can access it;
 - ii. information is accurate and suitable for the purpose for which it is processed; and
 - iii. authorised persons can access information if they need it for authorised purposes only.
 - iv. Personal information may not be stored on individual computers, phones or



other IT devices but instead on our Office computer and or Manager Dedicated Laptops. Personal information held in hard copy is only permitted where OCOSC can demonstrate a legitimate interest under GDPR, recorded, distributed and retained in accordance with Annex A & B of this policy.

- c. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.
- d. Personal information must not be transferred to any person to process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.
- e. Security procedures include:
 - i. **Physically securing information.** Any desk or cupboard containing confidential information must be kept locked. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
 - ii. **Controlling access to premises.** Staff should immediately report to the Manager/Deputy manager of the site if they see any person they do not recognised in any of the entry-controlled areas listed below
 - a. Main Office cupboard
 - b. Main site Foyer cupboard
 - c. OCOSC Safe
 - d. OCOSC Attic
 - e. Christ Church Documentation Cupboard
 - f. Chester park documentation Cupboard
 - iii. **Telephone Precautions.** Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:
 - a. the identity of any telephone caller must be verified before any personal information is disclosed;
 - b. if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;
 - c. do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.
 - iv. **Methods of disposal.** Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.
 - v. **Additional measures to ensure data security include**
 - a. Photocopying done off site will be supervised at all times by a member of staff/director/trustee
 - b. OCOSC administration carried out by a member of staff/director/trustee



offsite such as individuals homes. The individual's home is considered to be an extension of the OCOSC office and falls under this policy. The handling of Data and its security shall conform to this policy.

9. Subject access requests

- f. By law, any Subject (including Staff) may make a formal request for information that we hold about them, provided that certain conditions are met. The request must be made in writing. In some circumstances it may not be possible to release the information about the Subject to them eg if it contains personal data about another person.
- g. Any member of staff who receives a written request should forward it to the Data Protection Officer immediately.

Signed for and on behalf of OCOSC:	{hard copy Signed}
Name of signatory (capitals):	...GP Thompson...
Reviewed on:	...23 May 2018.....
Next review due:	...23 May 2019 ...



Annex A to OCOSC Data Protection and Data Security Policy

Issue	The Directive	The GDPR	Impact
Lawful basis Under EU data protection law, there must be a lawful basis for all processing of personal data (unless an exemption or derogation applies).	Rec.30; Art.7(1) Personal data may be processed only if at least one lawful basis applies.	○ Rec.39, 40, 41; Art.6(1) Personal may be processed only if, and to the extent that, at least one lawful basis applies.	= The obligation on organisations to have a lawful basis in respect of each processing activity is essentially unchanged.
Consent Personal data may be processed on the basis that the data subject has consented to such processing.	Rec.30, 33; Art.7(1)(a) Processing is permitted if the data subject has consented to the processing.	⊗ Rec.32, 42, 43; Art.6(1)(a) Processing is permitted if the data subject has consented to the processing.	= "Consent" remains a lawful basis for processing personal data. However, under the GDPR, valid consent becomes significantly harder to obtain (see Chapter 8).
Contractual necessity Personal data may be processed on the basis that such processing is necessary in order to enter into or perform a contract with the data subject.	Rec.30; Art.7(1)(b) Processing is permitted if it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his or her request prior to the entry into a contract.	○ Rec.44; Art.6(1)(b) Processing is permitted if it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his or her request prior to the entry into a contract.	= "Contractual necessity" remains a lawful basis for processing personal data.
Compliance with legal obligations	Rec.30; Art.7(1)(c) Processing is permitted if it is	○ Rec.45; Art.6(1)(c), 6(3) Processing is permitted if it is necessary for	= "Compliance with legal obligations" remains a lawful basis for



Personal data may be processed on the basis that the controller has a legal obligation to perform such processing.	necessary for compliance with a legal obligation.	compliance with a legal obligation under EU law or the laws of a Member State.	processing personal data. ⊖ The fact that this legal basis is explicitly limited to legal obligations arising in the EU may place organisations that are subject to non-EU court orders to disclose data in a difficult position.
Vital interests Personal data may be processed on the basis that it is necessary to protect the "vital interests" of the data subject (this essentially applies in "life-or-death" scenarios).	Rec.31; Art.7(1)(d) Processing is permitted if it is necessary in order to protect the vital interests of the data subject.	⊗ Rec.46; Art.6(1)(d) Processing is permitted if it is necessary in order to protect the vital interests of the data subject or of another natural person.	⊕ Under the GDPR, the "vital interests" processing condition can extend to other individuals (e.g., children of the data subject). This is a helpful clarification.
Public interest Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.	Rec.32; Art.7(1)(e) Processing is permitted if it 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.	○ Rec.45; Art.6(1)(e) Processing is permitted if it 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.	⊖ "Public interest" remains a lawful basis for processing personal data. Note also that processing carried out on this basis may be subject to objections from data subjects (see Chapter 9).
		⊗	⊖



Legitimate interests Personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.	Rec.30; Art.7(1)(f) Processing is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party to whom the data are disclosed) except where the controller's interests are overridden by the interests, rights or freedoms of the affected data subjects.	Rec.47, 48; Art.6(1)(f) Processing is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child. This does not apply to processing carried out by public authorities in the performance of their duties.	"Legitimate interests" remains a lawful basis for processing personal data. Note also that processing carried out on this basis may be subject to objections from data subjects (see Chapter 9). – Parental permission is required to process the personal data of children (and note that a child is anyone under the age of 16). In some contexts (especially online) proving that parental permission has been obtained may be difficult.
Processing Sensitive Personal Data The processing of Sensitive Personal Data is only permitted under certain conditions:	Rec.34; Art.8 The processing of Sensitive Personal Data is prohibited, unless:	⊗ Rec.51-56; Art.9 The processing of Sensitive Personal Data is prohibited, unless:	+ The changes introduced by the GDPR are positive for most organisations, because they provide additional grounds on which Sensitive Personal Data may lawfully be processed.
• Explicit consent	• Art.8(2)(a) The data subject has given explicit consent.	• Art.9(2)(a) The data subject has given explicit consent.	



• Employment law	• Art.8(2)(b) The processing is necessary in the context of employment law.	• Art.9(2)(b) The processing is necessary in the context of employment law, or laws relating to social security and social protection.	
• Vital interests	• Art.8(2)(c) The processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving consent.	• Art.9(2)(c) The processing is necessary to protect vital interests of the data subject (or another person) here the data subject is incapable of giving consent.	
• Charity or not-for-profit bodies	• Art.8(2)(d) The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, or persons with whom it has regular contact in connection with its purposes.	• Art.9(2)(d) The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes.	



Data manifestly made public by the data subject	Art.8(2)(e) The processing relates to personal data which have been manifestly made public by the data subject.	...Art.9(2)(e) The processing relates to personal data which have been manifestly made public by the data subject.	
Legal claims	Art.8(2)(e) The processing is necessary for the establishment, exercise or defence of legal claims.	...Art.9(2)(f) The processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.	
Reasons of substantial public interest	N/A	Art.9(2)(g) The processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects.	
Medical diagnosis and treatment	Art.8(3) The processing is required for the purpose of medical treatment undertaken by health professionals.	Art.9(2)(h), (3) The processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity	



		of employees and the management of health or social care systems and services.	
Public health	N/A	Art.9(2)(i) The processing is necessary for reasons of public interest in the area of public health (e.g., ensuring the safety of medicinal products).	
Historical, statistical or scientific purposes	N/A	Art.9(2)(j) The processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.	
Exemptions under national law	Subject to appropriate safeguards, Member States may, for reasons of public interest, lay down additional exemptions.	Art.9(4) Member States may maintain or introduce further conditions, including limitations with regard to genetic data, biometric data or health data.	
Processing for new purposes	Art.6(1)(b), 13(1)	⊗ Rec.50; Art.6(4)	⊖ The Directive permits the processing of



Notwithstanding the "data minimisation principle" (see Chapter 6) there are some circumstances in which personal data may be processed for new purposes that go beyond the original purpose for which those data were collected.	Personal data may be processed for new purposes, provided that those new purposes are "not incompatible" with the original purpose. Member State law may permit processing for new purposes (beyond the original purpose) if this is a necessary measure to safeguard special public interests (e.g., national security, defence, public security, etc.).	Where personal data are to be processed for a new purpose, the controller must consider whether the new purpose is "compatible" with the original purpose taking into account the following factors: • any link between the original purpose and the new purpose; • the context in which the data have been collected, including the controller's relationship with the data subjects; • the nature of the personal data, in particular, whether Sensitive Personal Data are affected; • the possible consequences of the new purpose of processing for data subjects; and • the existence of appropriate safeguards (e.g., encryption or pseudonymisation).	personal data for new purposes, provided that those new purposes are "not incompatible" with the original purpose. This is a reasonably low bar. However, the GDPR makes it harder for organisations to process personal data for new purposes, because the task of determining which new processing purposes are "compatible", and which are not, is an onerous one. + The fact the GDPR recognises that pseudonymisation reduces the level of risk involved in processing personal data is a positive development for organisations that routinely process pseudonymised data (e.g., clinical trials companies).
---	--	---	---



Processing not requiring identification In some circumstances, controllers have an obligation to retain certain data for the purposes of compliance with applicable law.	N/A The Directive does not directly address this issue.	 Rec.57; Art.11(1) If the purposes for which the controller is processing the personal data do not require the identification of the data subject, the controller is not required to maintain information identifying the data subject in order to comply with the GDPR.	 The GDPR helpfully clarifies the fact that controllers are not required to retain information that identifies data subjects solely for the purposes of complying with the GDPR.
--	---	---	--



Annex B to OCOSC Data Protection and Data Security Policy



Document	Data subject and approximate number of data subjects	Data recorded, including special categories of data	Lawful basis for recording data including conditions for special categories of data	Data sharing/ recipients	Data storage. Safety precautions. Data Processor (app, if used)	Data retention	Data destruction
Child Record of Information	Child, parents/carers. Family members/ emergency contact person/ approximate number- 800	Information about the child. Contact details of parents. Where the child lives and with whom they reside. Parental responsibility and emergency contact details	Legal obligation GDPR6(1)(c) Safeguarding and Welfare Requirement of the statutory framework: EYFS 2017, 3.5	Data shared with Ofsted as the regulator. Shared with the LADO, the police, Children's Social Services and legal services	As detailed in our policy	Until child is 21 years and 3 months, in the case of litigation and to comply with the Limitation Act 1980	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Attendance Register	Children and childminding assistants approximate number- 300	Child's arrival and departure time. Name of childminder assistant/s in attendance.	Legal obligation GDPR6(1)(c) Requirement of the statutory framework: EYFS 2017 3.76 Childcare Register 2016	On the request of Ofsted, police, legal services	As detailed in our policy	Until child is 21 years and 3 months in the case of litigation to comply with the Limitation Act 1980	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Accident, Injury (including existing injuries) Administration of Medicine records and Physical Intervention log	Child. Parent/carers. approximate number- 300	Child's personal information, staff names and parent name and signature	Legal obligation GDPR6(1)(c) Safeguarding and Welfare Requirement of statutory framework: EYFS 2017, 3.50, 3.46 and Childcare Register 2016 Also on the basis of 'vital interests' GDPR 6(1)(d) and	On the request of Ofsted and emergency services.	As detailed in our policy	Until child is 21 years and 3 months in the case of litigation to comply with the Limitation Act 1980	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.



			'legitimate interests' GDPR 6(1)(f)				
Welfare/ safeguarding concerns about a child	Child. Parents or carers. Could be family members or other. approximate number- 800	Sensitive information on child or family, parents' names and child's name	Legal obligation requirement of the statutory framework EYFS 2017, 3.5	For safeguarding purposes the data may be shared with Ofsted and other agencies including the LADO, Children's Social Services, the police, legal services	As detailed in our policy	Record should be passed to next setting in line with Keeping Children Safe In Education.	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Complaints Log	Complainant	Child and family details, provider details, sensitive information	Legal obligation GDPR6(1)(c) Requirement of the statutory framework: EYFS 2017, 3.74 and Childcare Register 2016	The log must be made available to Ofsted	As detailed in our policy	Retention for 3 years, see Childcare Register Requirements CR 7.3	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Consent forms	Child and parent/carers approximate number- 800	Child and parent names and signatures of parent and setting	Legal obligation GDPR 6(1)(c) to work in partnership under the EYFS 2017 statutory framework plus 'legitimate interest' 6(1)(f) to provide high quality setting.	Document may be shared with Ofsted and legal services in the case of litigation	As detailed in our policy	Until child is 21 years and 3 months	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Childcare business contracts	Parent/carers approximate number- 300	Contract details between parent and provider.	Contractual necessity for public liability insurance. GDPR6(1)(b)	The document may be shared with HMRC or legal services	As detailed in our policy	For at least 5 years after the 31 st January submission deadline for relevant tax year	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.



Learning and development observations and summative assessments including 'all about me' two year progress check, transfer records	Child approximate number- 300	Photographs, comments and judgements on child's learning, skills and disposition and presentation	Legal obligation GDPR 6(1)(c) Learning and Development Requirements of the statutory framework EYFS 2017. Also 'legitimate interest' GDPR 6(1)(f) to track development effectively. Photo consent can be withdrawn at any time	Shared with Ofsted on request. Shared only with parental consent with Health Visitor, Speech and Language Therapist, SENCO, health professional	As detailed in our policy	Until a child starts school or leaves to attend a new setting	Documents deleted and storage devices wiped clean after a reasonable period of time to allow childminder to forward the information to parents and the receiving setting.
Local authority funding form	Child approximate number- 300	Child and family personal information including NI details, DOB, eligibility for two year old funding and EYPP codes and 30hour codes	Contractual obligation as required by LA for funding requirements GDPR6(1)(b)	Shared with Ofsted and Dept. for Education	Pioneer system. Password protected. Password changed every 30 days.	Information held on Pioneer as per local authority retention period	Information held on Pioneer as per local authority retention period
Notifications to Ofsted	Members of family/household. Childminding assistant. approximate number- 800	Changes to household and staff. Sensitive information relevant to suitability of anyone in household or assistants including health and criminal convictions	Legal obligation GDPR6(1)(c) as required by the Safeguarding and Welfare Requirements statutory framework of the EYFS 2017 3.77	Data may be shared with Ofsted, LADO, police	As detailed in our policy	Three years or until next Ofsted inspection	Documents deleted and storage devices wiped clean after the required period of time
Policies and procedures – acknowledgement of receipt, including receipt of Privacy Notice	Parent/carer approximate number- 300	Parent confirmation that policies have been read and understood. Child details and parent and setting signatures	Legitimate interest GDPR 6(1)(f) to provide a high quality service, following the principle of parent partnership in EYFS. Privacy Notice is a	Document may be Ofsted and ICO	As detailed in our policy	Deleted once child moves to another setting	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.



			legal obligation under GDPR				
Visitors' log	Visitors to household	Date of visit, visitor name, reason for visit and times arriving and departing	Legitimate interest to safeguard children GDPR 6(1)(f)	Document may be shared with Ofsted or police	As detailed in our policy	Until next Ofsted inspection	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Financial Records /HMRC	Parents. Childminding assistant approximate number- 300	Invoices and receipts with parents' and child's name.	Legal obligation required by HMRC GDPR6(1)(c)	On request by HMRC	Purchase receipts kept securely. As detailed in our policy	For at least 5 years after the 31 st January submission deadline of the relevant tax year	Documents deleted or wiped clean on storage devices. Paper documents shredded after the required length of time.
Staff records	Childminding assistants. approximate number- 20	Name of staff member Address Telephone Emergency contact numbers Application form	GDPR 6(1)(b) – The processing is necessary for the performance of a contract with the data subject. GDPR 6(1)(f) – necessary for the purposes of legitimate interests	Data shared with Ofsted on request of inspector. HMRC inspector. LADO in the case of safeguarding matters	As detailed in our policy	<i>Financial records should be retained for 6 years</i>	<i>Financial records should be retained for 6 years</i>



		References Employment history Qualifications Notes on responses to Interview questions Identity checks Medical suitability and medical requirements DBS number Permission to work in UK, if required – Nat Insurance number Declaration on Disqualification and Disqualification by Association Signed Confidentiality Agreement Copies of letters which have been sent to the staff member, such as invitation to interview/ letter of job offer Contract - terms of employment/contracted hours etc. Induction checklist Record/notes from supervision sessions	pursued by the controller. Legal obligation GDPR6(1)(c) - in relation to financial/HMRC records <i>GDPR 9(2)(a) – Explicit consent of the data subject for any data on race, ethnicity, religion, health, special needs, sexual orientation</i> <i>Criminal convictions should be notified to Ofsted. GDPR Legal obligation GDPR6(1)(c) and Article 10 for holding data on criminal convictions</i>				
--	--	---	---	--	--	--	--



		Annual appraisal forms					
		Record of holidays booked					
		Payment details					
		Bank account details					



Annex C to OCOSC Data Protection and Data Security Policy

Consent Form enabling OCOSC to retain and use Data in accordance with the OCOSC Data Protection and Data Security Policy

I (insert full name)

Am aware of the existence of the OCOSC Data Protection and Data Security Policy. The policy is held in the policy file, at each of the sites (where OCOSC provide a service) and is available via the OCOSC website.

I have read the policy and understand that the Data collected by OCOSC, is required by OCOSC, in order that they can provide Breakfast, Afterschool and Holiday club services and has been collected with my consent.

I confirm that the data provided by me to OCOSC, concerning my partner, emergency contacts and children has been provided with their knowledge and consent and I have made them aware of OCOSC policy and its availability via the Website.

The Data collected will be retained, used, distributed and destroyed in accordance with this policy.

I give consent, where a legal obligation is placed upon OCOSC, to share my data with 3rd parties (for example Ofsted, Child protection Agencies, HM revenue, Company house, Charity commission, School etc.)

I do not consent to OCOSC sharing my data with 3rd parties, in any situation, where there is no legal requirement, without my explicit written permission which shall be obtained in advance.

I understand that any data shared will be used for the sole purpose for which it was given only. OCOSC has an obligation under this policy to ensure that the 3rd party concerned has an appropriate policy in place that protects the use and security of my data.

Signed _____

Name _____

Date _____