Policy Ref:

 # GOV15

Somerset Activity & Sports Partnership

Data Protection Policy

Date Approved	October 2024
Approved By	SMT
Review Date	October 2026

Policy Update Record (Version Control)		
Date	**Author**	**Change(s)**
16/09/2024	Rachel Martin	Policy re-formatted and updated.

Contents

Introduction

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an organisation we will collect, store and process personal data about our participants (including parents of participants if under 18 years of age), clients, workforce, and others. This makes SASP a data controller in relation to that personal data.

We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines and reputational penalties for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in penalties being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

About this policy

The types of personal data that we may be required to handle include information about participants, parents, our workforce (including staff, volunteers and trustees) and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('GDPR'), the Data Protection Act 2018, and other regulations (together 'Data Protection legislation').

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Definition of data protection terms

A list of definitions is included in **Appendix 1.1** of this policy.

Data Protection Officer (DPO) / Data Protection Lead (DPL)

SASP aren't required to appoint a DPO under the UK GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO and we support our DPO to the same standards.

DPO: Rachel Martin – rmartin@sasp.co.uk

The DPO is responsible for ensuring compliance with the Data Protection legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

SASP Responsibilities

SASP is committed to protecting and respecting the confidentiality of sensitive information relating to participants, staff, and trustees. SASP will:

a) Follow the key principles of Data Protection legislation including the 7 principles of GDPR (**see Appendix 1.2**);
b) register with the Information Commissioners Office (ICO);
c) keep an up-to-date Information Asset Register (IAR) which lists all known stores of personal data in the organisation, alongside a Record of Processing Activity (RoPA) which lists all known instances of data processing, including the lawful basis for processing under Data Protection legislation, who it is shared with, where it is stored (including transfer out of the UK) and how long it is retained for.
d) verify that all systems that involve personal data or confidential information will be examined to see that they meet Data Protection regulations (see **Data security**)
e) inform all users about their rights regarding data protection;
f) provide training to ensure that staff know their responsibilities;
g) monitor its data protection and information security processes on a regular basis, changing practices if necessary (see **Data security**).

Responsibilities of Staff, Volunteers and Trustees

All staff, volunteers and Trustees are responsible for checking that any information that they provide to SASP is accurate and up to date.

All staff are responsible for ensuring that any personal data they use in the process of completing their role:

a) is not in the view of others who do not have the authority to view the data;
b) is kept securely in a locked cabinet when not being used;
c) is stored on a secure local or network drive;
d) if on a SASP PC or laptop, that the device is locked when the staff member is out of the room;
e) if kept on removable storage (laptop, tablet, USB memory stick) approved by SASP, that this is password protected and encrypted. The data held on these devices must be backed up regularly and this is the responsibility of the individual;
f) is not disclosed to any unauthorised third party (this includes verbal disclosures of confidential information);
g) is assessed and approved by the Senior Management Team (SMT) or the DPO.

Staff should follow the security measures set out in the **Data security** section of this policy.

Staff will report any loss, theft or mishandling of personal data promptly to the DPO.

Staff should note that unauthorised disclosure or transgression of the above statements or security measures in may result in disciplinary or other action.

Staff should ensure that they use the email address provided by SASP for **only** work-related business and communication. All communication remains the property of SASP and may be disclosed as part of a Subject Access Request (**see Appendix 5**).

Staff will follow the email retention policy as laid out in the **Data Retention** section of this policy.

When staff leave SASP, they are required to hand over all personal data belonging to SASP. They must not remove any personal data without permission from SASP. Taking personal data with no lawful basis may be a criminal offence.

Participants (and Parents/Guardians - Seeking Consent)

If consent is required for the processing of personal data of any participant, then the form of this consent must:

a) inform the data subject of exactly what we intend to do with their personal data
b) require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
c) inform the data subject of how they can withdraw their consent.
d) Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

SASP will generally seek consent to process personal data directly from a participant who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore it may be required to seek consent from an individual with parental responsibility. For any participants under the age of 12, the consent of a Parent/Guardian will always be sought.

Separate consent will also be sought regarding matters of use of personal data such as the use of images and names in publicity materials on induction or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

Rights of the data subject

All people having personal data stored by SASP have the right to:

a) obtain confirmation if personal data concerning him or her (or their child) is being processed;
b) Where this is the case, have a copy of the personal data and the following information:
- the purposes of the processing;
- the third parties that the data will be shared with;
- the period for which the personal data will be stored;
- the existence of the right to request from SASP to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held;
- the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from the data subject, any available information as to its source.

c) if exemptions are placed on any of the data above, because of safeguarding or other issues, the existence of this data will be declared.

SASP will place on its website a Privacy Notice regarding the personal data held about participants and why it is processed. Privacy Notices for workforce and trustees will be distributed to data subjects and be held on the Staff Intranet.

Access to the data is called a **Subject Access Request (SAR)**. Any person who wishes to exercise this right (or their parental right) should make a request (which does not need to be in writing) and submit it to the DPO. The process for dealing with a Subject Access Request is

outlined in **Appendix 5**.

SASP will respond to requests for access to personal information within one calendar month and in accordance with advice from the ICO and other professional agencies.

For further information on how SASP upholds the rights of the data subject please see **Appendix 1.3.**

Freedom of Information Request

The Freedom of Information Act (FOIA) doesn't generally apply to charities, but information on any services SASP supply on behalf of a public authority, could be requested under the FOIA.

In this event, the public authority is responsible for responding to the request, and for deciding whether the information can be released to the public. SASP must support them by providing any information that they'll need for their reply.

Data security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures include:

a. **Entry controls.** The main offices are kept locked. Any stranger seen in the offices should be reported to the Data Protection Officer.
b. **Staff network and software permissions.** Staff will only have the level of permissions required for their role. When staff leave SASP, all their permissions and accounts will be deleted.
c. **Data walks.** The DPO conducts an annual data walk to assess the risk of data loss around the site, including physical security. The record of the walk and findings forms part of our monitoring documentation.
d. **Data on display.** All personal data on display has been assessed for risk and minimised where necessary. Consent has been sought for display where we do not have a legal, public interest, or legitimate interest in displaying the personal data.
e. **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind, or information which would cause distress or harm if it was disclosed.
f. **Privacy Impact Assessments.** In line with Data Protection legislation, SASP will carry out a Privacy Impact Assessment when using software or online tools which may, if breached, cause harm to the rights and freedoms of individuals. These risk assessments will be carried out with the support of the DPO (see **Appendix 4 Privacy Impact Assessment).** The risk of data being transferred in and out of the UK will also be assessed.
g. **Methods of disposal.** Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required. IT assets are disposed of in accordance with the ICO's guidance on the disposal of IT assets via our IT Support Providers.
h. **Data retention**. To minimise the risk of data being lost or mishandled, we will not retain data including emails any longer than is required by law or where there is a business need. See **Data retention** section.

i. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended.
j. **Working away from the office – paper documents.** Confidential documents should not be removed from the premises. On occasion it may be necessary to take documents off-site that contain other information, i.e. minutes for off-site meetings. Staff should ensure that they keep these documents safely and return them to the office as soon as possible.
k. **Working away from the office – electronic working**. Confidential information should not be saved to the C Drive, Hard Drive or memory Sticks. Staff should only use a secure network, i.e. the OneDrive/SharePoint if it is necessary to work on confidential information off-site. All staff are provided with a laptop and/or tablet/phone, confidential information should not be downloaded onto personal devices.
l. **Document printing.** Documents containing personal data must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Data Breaches

If there is a data breach staff will inform the DPO who will then advise on any actions.

Any data breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken as shown in **Appendix 7**.

If there is judged to be a significant risk to the rights and freedoms of the affected data subject, SASP will communicate the breach to the data subjects with the support of the DPO.

In the case of a personal data breach where there is a significant risk of harm to the rights and freedoms of data subjects, the ICO should be informed as soon as possible and **within 72 hours of notification**. Further investigation of the breach can take place after this notification in line with advice from the DPO and the ICO.

Data breaches are reported using the information found at on the ICO website https://ico.org.uk/for-organisations/report-a-breach/ and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

When reporting a breach, Data Protection legislation states that we must provide:

a. description of the nature of the personal data breach including, where possible:
b. the categories and approximate number of individuals concerned; and
c. the categories and approximate number of personal data records concerned;
d. the name and contact details of the data protection officer or other contact point where more information can be obtained;
e. description of the likely consequences of the personal data breach; and
f. description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Data Retention (including emails)

SASP has responsibilities under the Data Protection Principles to keep data only for as long as necessary.

SASP has a clear email retention policy. Emails containing personal information of participants which may be required for participation in a project/programme or safeguarding purposes are transferred to/collated into an appropriate database and permanently deleted from our email system. This data is stored securely for the length of the project/programme (and beyond this if needed for reporting/auditing purposes – which will be made clear in the privacy notice for the project/programme).

Emails containing the personal information of staff members are attached to the staff members electronic personnel file and permanently deleted from our email system.

Staff are reminded to tidy their emails periodically.

If paper is due to be destroyed it will be cross-cut shredded either by SASP or by a commercial company. SASP will request and retain a certificate of destruction issued by any third party.

If data is held on electronic devices then this will be deleted in line with the advice from the ICO.

Reporting Policy Incidents

Any member of staff, participant or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the DPO.

Monitoring and evaluation

This policy will be monitored and reviewed in line with the policy review schedule.

Appendix 1.1 Data Protection terms and definitions

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes participants, our workforce, volunteers, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection legislation. We are the data controller of all personal data used in our business for our own commercial & operating purposes.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data Users	Those of our workforce (including trustees and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Information Asset Register	The inventory of all the data storage locations used by SASP.
Personal Data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Register of Processing Activity (RoPA)	The register of all the data processed by SASP including the lawful basis for processing, who it is shared with, where it is transferred (including out of the UK) and how long it is retained for.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

Appendix 1.2: Data Protection principles

Anyone processing personal data must comply with the data protection principles.

These provide that personal data must be:

- processed fairly and lawfully and transparently in relation to the data subject
- processed for specified, lawful purposes and in a way which is not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date
- not kept for any longer than is necessary for the purpose
- processed securely using appropriate technical and organisational measures.

Personal data must also:

- be processed in line with data subjects' rights (see Appendix 1.3)
- not be transferred to people or organisations situated in other countries without adequate protection.

Appendix 2: Rights of the data subject and how we uphold them

1. **The right to be informed:** Data subjects are informed of how we process their personal data through Privacy Notices at the point of giving data, or by relevant 3rd parties in cases where referrals are being made on their behalf by a medical professional.

2. **The right of access:** Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with SASP's Subject Access Request Procedure – See Appendix 5.

3. **The right to rectification:** If a data subject informs SASP that personal data held about them is inaccurate or incomplete then we will consider that request and provide a response within one month. If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case. Whilst we will endeavour to ensure that all data held about a data subject is correct, we may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the ICO at the time that we inform them of our decision in relation to their request. Some examples of where a request for rectification may be rejected is if it is deemed to be manifestly unfounded (lack of evidence proving inaccuracy), excessive (rectification requested multiple times with no new evidence being provided), if SASP have a legitimate interest in keeping the data in its current form for legal/regulatory reasons, or where the data is opinion-based (proving inaccuracy is impossible).

4. **The right to erasure**: Data subjects have a right to have personal data about them held by SASP erased only in the following circumstances.
   - Where the personal data is no longer necessary for the purpose for which it was originally collected.
   - When a data subject withdraws consent – which will apply only where SASP is relying on the individuals consent to the processing in the first place.
   - When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.
   - Where the processing of the personal data is otherwise unlawful.
   - When it is necessary to erase the personal data to comply with a legal obligation.

   SASP is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:
   - to exercise the right of freedom of expression or information
   - to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
   - for public health purposes in the public interest
   - for archiving purposes in the public interest, research or statistical purposes
   - in relation to a legal claim.

   If SASP has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort. The DPO must be consulted in relation to requests under this right, and a response issued to the data subject within one calendar month of the request being submitted.

5. **The right to restrict processing**: Data subjects have a right to 'block' or suppress the processing of personal data. This means that SASP can continue to hold the personal data but not do anything else with it. SASP must restrict the processing of personal data:

- where it is in the process of considering a request for personal data to be rectified (see above)
- where SASP is in the process of considering an objection to processing by a data subject
- where the processing is unlawful, but the data subject has asked SASP not to delete the personal data
- where SASP no longer needs the personal data, but the data subject has asked SASP not to delete the personal data because they need it in relation to a legal claim, including any potential claim against SASP.

- If SASP has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort. The DPO must be consulted in relation to requests under this right, and a response issued to the data subject within one calendar month of the request being submitted.

6. **The right to data portability**: In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation. This right doesn't extend to data provided by third parties or data that was initially provided in a non-electronic format (like paper forms) and then entered into an automated system. If such a request is made, then the DPO must be consulted, and a response issued to the data subject within one calendar month of the request being submitted. This right may be rejected by SASP if it is deemed it will have an impact on third-party rights or impair the ability for SASP to process the data for legitimate purposes.

7. **The right to object**: In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest. An objection to processing does not have to be complied with where SASP can demonstrate compelling legitimate grounds which override the rights of the data subject. Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right, and a response issued to the data subject within one calendar month of the request being submitted. In respect of direct marketing any objection to processing must be complied with. SASP is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

8. **Rights in relation to automated decision making and profiling:** SASP will carefully consider whether it takes any decisions about any individuals by automated means. This includes any decisions made solely by automated means, and which has a legal effect in relation to the individual. This might include, for example, a decision as to whether to employ an individual. We consider it to be unlikely that this would apply to SASP as there is always likely to be an element of human intervention in any decision making. However careful consideration should be given to this issue.

Appendix 3: Role of the Data Protection Officer

Purpose
The Data Protection Officer (DPO) is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee and verify SASP's data protection processes and advise on best practice.

Data Protection Officer Responsibilities
To:

- advise SASP about their obligations under the General Data Protection Regulation 2016 and the Data Protection Act 2018;
- develop a joint understanding of SASP's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- monitor SASP's compliance with data protection law, by:
  - collecting information to identify data processing activities;
  - analysing and checking the compliance of data processing activities;
  - informing, advising and issuing recommendations;
  - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- Ensure that policies are followed, through:
  - assigning responsibilities to individuals;
  - awareness-raising activities;
  - coordinating staff training;
  - conducting internal data protection audits;
- advise on and assist with carrying out data protection privacy impact assessments, if necessary;
- act as a contact point for the ICO, assisting and consulting it where necessary, including:
  - helping the ICO to access documents and information;
  - seeking advice on data protection issues;
- act as a contact point for individuals whose data is processed (for example, staff, participants and parents), including:
  - responding to subject access requests;
  - responding to other requests regarding individuals' rights over their data and how it is used;
- take a risk-based approach to data protection, including:
  - prioritising the higher-risk areas of data protection and focusing mostly on these
  - advising SASP if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve.
- report to the board of trustees on SASP's data protection compliance and associated risks;
- respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role;
- maintaining a record of SASP's data processing activities;
- work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security;
- work with the Senior Management Team to ensure GDPR compliance;
- assist with any additional tasks necessary to keep SASP compliant with data protection law

Tasks

From these responsibilities, isolated tasks should include:

- providing a model Data Protection Policy and assist in customising it for SASP;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- providing advice on other associated policies and documents;

- providing materials and advice in completing a dynamic Information Asset Register and assisting in its completion if necessary;
- providing training materials to assist staff in keeping up to date with Data Protection issues;
- acting as the point of contact for SAR and FOI requests and supporting SASP to provide the information as required;
- providing a Data Protection Audit on a 3 yearly rota basis and producing a report for the Board of Trustees;
- providing telephone and email advice and support;

Appendix 4: Privacy Impact Assessment

Before the use of any new service that uses personal data, staff should fill in a Privacy Impact Assessment Form.

The SMT, with advice from the DPO, will then approve the use and the information be placed on the Information Asset Register.

Important points to consider:

Data Protection Principles

- processing to be lawful and fair
- purposes of processing be specified, explicit and legitimate
- adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is necessary
- processed in a secure manner

Why we need a Privacy Impact Assessment – screening questions

We need to complete this form because:

- the use involves the collection of new information about individuals;
- the use compels individuals to provide information about themselves;
- the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information;
- we are using information about individuals for a purpose it is not currently used for, or in a way it is not currently used
- we are using new technology that might be perceived as being privacy intrusive, for example, the use of biometrics or facial recognition;
- the use results in us making decisions or acting against individuals in ways that can have a significant impact on them;
- the information about individuals is of a kind particularly likely to raise privacy concerns or expectations, for example, health records, criminal records or other information that people would consider to be private;
- the use requires us to contact individuals in ways that they may find intrusive.

Privacy Impact Assessment Form

Name of Service/Software/App
Describe the service
Describe the data collected and the possible uses of the data

List of data held	**Collection of data**
	Possible uses

Identify the privacy, related risks and possible solutions			
Privacy issue	Risk to individuals	DPA (Data Processing Agreement) Risks	Possible Solutions

Comments on risks	Processes that must be in place

Sign off and notes
PIA Contact Name/Email (Lead for service/software/app)
Date Completed

Please submit this form to the DPO

SMT / DPO Approval Notes
Date Approved

Appendix 5: Subject Access Request (SAR) Process

On receiving a Subject Access Request or request for change or deletion of data the DPO will:

- inform the SMT;
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- contact the ICO if clarity on the request or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **one calendar month**, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Subject Access Requests are held here: SASP Wellington Offices – GDPR File

Subject Access Request Record

Name of data subject:
Date request received:
Date acknowledgement sent:
Name of person(s) dealing with request:

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, ask third parties to release external data.
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?
Date request completed:	(within 30 days of request)
Signed off by:	

Appendix 6: Data Breach Process

Every Data Protection Breach should be recorded. The process that should be followed is listed below:

- inform the DPO

- record the details of the breach providing these details:
  - a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
  - the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Contact the DPO if clarity on reporting the breach is needed and if necessary, the DPO may report to the ICO;

- either by phoning 0303123 1113
- By filling in the form at: https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc and sending it to casework@ico.org.uk

The DPO or SMT will then:

- update this record where necessary (see next page);
- identify the people whose data is accidentally released, inform them of the breach and the processes taken to rectify the situation;
- review why the breach took place and if future similar events can be avoided.

The Data Protection Breach records are held here: Wellington Offices – GDPR File

Data Breach Record

Date of Breach	Name of person reporting the breach
Description of the nature of the personal data breach – how it occurred	
The categories and approximate number of individuals concerned	
The categories and approximate number of personal data records concerned	
A description of the likely consequences of the personal data breach	
A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects	
Date of Form/Submitted to DPO	

To be completed by the DPO / SMT

SMT Informed?	y/n	Is this high risk?	y/n	Report to ICO	y/n
Date reported to data subjects					
Notes					
Actions approved by			Date		