DATA PROTECTION
POLICY & PROCEDURES

Policy Title	Data Protection
Author/Job Title	Jonathan Sutton / CEO
Policy Version	Version Rev 2.2 (inc GDPR)
Status	Live
Reference and guidance	ICO guidance
Consultation Forum	Selected staff
Date of Consultation	9 May – 18 May 2018
Approving Body	Board of Trustees
Approval Date	No 3 Board 21 June 2018
Review Date	1 December 2018
Last Amendment Date	1 October 2020
Amended By	CEO
Available on external website	Yes
Available on intranet / Breathe HR	Yes
Role responsible for this policy	Data Compliance Officer (CEO)

Date of change	Reason for change or amendment	Name of person and job title making change	Document version number
1 Oct 2020	Review following data breach and report to ICO	J Sutton CEO	2.2

DATA PROTECTION POLICY
FOR RESIDENTS, EMPLOYEES, VOLUNTEERS, CONSULTANTS

OVERVIEW

1. St Paul's takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

2. St Paul's is registered with the Office of the Information Commissioner;

   a. Organisation name: St Paul's Hostel.
   b. Registration reference: Z9152112.

3. St Paul's is not a public authority and we are not required to appoint a DPO due to the nature of our processing activities and we have decided not to appoint a DPO voluntarily because the same duties and responsibilities would apply had we been required to appoint a DPO. St Paul's has a Data Compliance Officer (DCO). This role held by the CEO because it reports to our highest level of management the Board of Trustees.

4. This policy applies to current and former employees, volunteers, residents and consultants or contractors. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or any contract for services) and any other notice we issue to you from time to time in relation to your data.

5. St Paul's Hostel has separate privacy notices in place in respect of residents, volunteers and employees. A copy of these can be obtained from Data Compliance Officer. They are also available in electronic format on our website.

6. St Paul's has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from Data Compliance Officer.

7. The company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from Data Compliance Officer. We will only hold data for as long as necessary for the purposes for which we collected it.

8. St Paul's is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

9. This policy explains how St Paul's will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, St Paul's.

10. This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by us at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, then St Paul's intends to comply with the 2018 Act and the GDPR.

DATA PROTECTION PRINCIPLES

11. Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

a. be processed fairly, lawfully and transparently;
b. be collected and processed only for specified, explicit and legitimate purposes;
c. be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
d. be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
e. not be kept for longer than is necessary for the purposes for which it is processed; and
f. be processed securely.

12. We are accountable for these principles and must be able to show that we are compliant.

HOW WE DEFINE PERSONAL DATA

13. '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

14. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

15. This personal data might be provided to us by you, or someone else (such as a former employer or your doctor, or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

16. We will collect and use the following types of personal data about you:

17. recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;

a. your contact details and date of birth;

b. the contact details for your emergency contacts;

c. your gender;

d. your marital status and family details;

e. information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;

f. your bank details and information in relation to your tax status including your national insurance number;

g. your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;

h. information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);

i. information relating to your performance and behaviour at work;

j. training records;

k. electronic information in relation to your use of IT systems/swipe cards/telephone systems;

l. your images (whether captured on CCTV, by photograph or video); and

m. any other category of personal data which we may notify you of from time to time.

HOW WE DEFINE SPECIAL CATEGORIES OF PERSONAL DATA

18. '**Special categories of personal data**' are types of personal data consisting of information as to:

a. your racial or ethnic origin;
b. your political opinions;

c. your religious or philosophical beliefs;

d. your trade union membership;

e. your genetic or biometric data;

f. your health;

g. your sex life and sexual orientation; and

h. any criminal convictions and offences.

19. We may hold and use any of these special categories of your personal data in accordance with the law.

HOW WE DEFINE PROCESSING

20. **'Processing'** means any operation which is performed on personal data such as:

a. collection, recording, organisation, structuring or storage;

b. adaption or alteration;

c. retrieval, consultation or use;

d. disclosure by transmission, dissemination or otherwise making available;

e. alignment or combination; and

f. restriction, destruction or erasure.

21. This includes processing personal data which forms part of a filing system and any automated processing.

HOW WILL WE PROCESS YOUR PERSONAL DATA?

22. St Paul's Hostel will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

23. We will use your personal data for:

a. performing the contract of employment (or services) between us;

b. complying with any legal obligation; or

c. if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

24. We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

25. If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

EXAMPLES OF WHEN WE MIGHT PROCESS YOUR PERSONAL DATA

26. We have to process your personal data in various situations during your Service Referral, during recruitment, employment (or engagement) and even following termination of your stay with us or the ending of your employment (or engagement).

27. For example:

a. to decide whether to employ (or engage) you;

b. to decide how much to pay you, and the other terms of your contract with us;

c. to check you have the legal right to work for us;

d. to carry out the contract between us including where relevant, its termination;

e. training you and reviewing your performance*;

f. to decide whether to promote you;

g. to decide whether and how to manage your performance, absence or conduct*;

h. to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;

i. to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;

j. to monitor diversity and equal opportunities*;

k. to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;

l. to monitor and protect the health and safety of you, our other staff, customers and third parties*;

m. to pay you and provide pension and other benefits in accordance with the contract between us*;

n. paying tax and national insurance;

o. to provide a reference upon request from another employer;

p. to pay trade union subscriptions*;

q. monitoring compliance by you, us and others with our policies and our contractual obligations*;

r. to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;

s. to answer questions from insurers in respect of any insurance policies which relate to you*;

t. running our business and planning for the future;

u. the prevention and detection of fraud or other criminal offences;

v. to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;

w. Process applications for Housing Benefit or application for any externally funded services and;

x. for any other reason which we may notify you of from time to time.

28. We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Chief Executive.

29. We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

a. where it is necessary for carrying out rights and obligations under employment law;

b. where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;

c. where you have made the data public;

d. where processing is necessary for the establishment, exercise or defence of legal claims; and

e. where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

30. St Paul's will process information about any criminal convictions to make sure a person is suitable for employment or volunteering or where processed for residents, to inform our Risk Management processes and make sure a person is suitable for our services.

31. We might process special categories of your personal data for the purposes in paragraph above which have an asterisk beside them. In particular, we will use information in relation to:

a. your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;

b. your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

c. your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

d. Criminal convictions of residents to assess suitability for services.

32. We do not take automated decisions about you using your personal data or use profiling in relation to you.

SHARING YOUR PERSONAL DATA

33. Sometimes we might share your personal data with third parties and agents to carry out our obligations under our contract with you or for our legitimate interests.

34. We require those parties to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

35. Our legitimate activities include payroll services for staff and law enforcement agencies in order to deter or prevent crime.

36. We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

HOW SHOULD YOU PROCESS PERSONAL DATA FOR ST PAUL'S?

37. Everyone who works for, or on behalf of, St Paul's has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

38. St Paul's Data Compliance Officer is responsible for reviewing this policy and updating the Board of Trustees on the data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

39. You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of St Paul's and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

40. You should not share personal data informally.

41. You should keep personal data secure and not share it with unauthorised people.

42. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

43. You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

44. You should use strong passwords.

45. Screensavers are to be enabled automatically and screen savers must be used when not at your desk.

46. Personal data should be encrypted before being transferred electronically to authorised external contacts.

47. Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

48. Do not save personal data to your own personal computers or other devices.

49. Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Compliance Officer.

50. Use bright red lever arch or ring binders for storage of ALL papers containing Personal Data and Special Category Data.

51. You should not take personal data away from St Paul's without authorisation from your line manager or the Data Compliance Officer.

52. Personal data should be shredded and disposed of securely when you have finished with it. Secure data sacks are provided in the workplace for this purpose.

53. You should ask for help from the Data Compliance Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

54. Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

55. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

HOW TO DEAL WITH DATA BREACHES

56. We have measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

57. If you are aware of a data breach you must contact Data Compliance Officer immediately or if during silent hours the Duty Manager. Keep any evidence you have in relation to the breach.

A real example of a data breach

The home address of an employee of an organisation in Worcester, was given to a service user in a service run by St Paul's Hostel.

A street homeless person staying in a local hotel while awaiting re-housing. An extension to this stay was agreed and payment was made by the other organisation, who administer funding. The booking reference was sent by insecure email to the St Paul's hostel employee followed by a second email that included the invoice.

The invoice contained the home address of the employee who made the booking used a personal credit card not a work credit card. The personal address of the employee was passed to the service user by mistake when the booking reference was given.

SUBJECT ACCESS REQUESTS

58. Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a

request you should forward it immediately to the Data Compliance Officer who will coordinate a response.

59. If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Compliance Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

60. There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

YOUR DATA SUBJECT RIGHTS

61. You have the right to information about what personal data we process, how and on what basis as set out in this policy.

62. You have the right to access your own personal data by way of a subject access request (see above).

63. You can correct any inaccuracies in your personal data. To do this you should contact Data Compliance Officer.

64. You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Data Compliance Officer.

65. While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Data Compliance Officer.

66. You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

67. You have the right to object if we process your personal data for the purposes of direct marketing.

68. You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

69. With some exceptions, you have the right not to be subjected to automated decision-making.

70. You have the right to be notified of a data security breach concerning your personal data.

71. In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Data Compliance Officer.

72. You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

PROCEDURES

THE PROCEDURE FOR MAINTAINING DATA SECURITY DURING TRANSMISSION TO A THIRD PARTY

73. St Paul's hostel takes the security and privacy of personal data seriously. A particular risk involves the loss of data between organizations. This procedure explains how St Paul's will reduce the risk of this happening and retrieve the data if it does. The following procedures are to be followed for all documents leaving St Paul's that contain Personal Data.

Transmission by e-mail

74. Word or other electronic documents. Completed documents containing Personal Data must be encrypted with a strong password. It is not necessary to encrypted for distribution within St Paul's.

75. The following must be followed;

a. Completed document must be encrypted with a strong password.[1]
b. The password is given to the recipient using a method other than email.

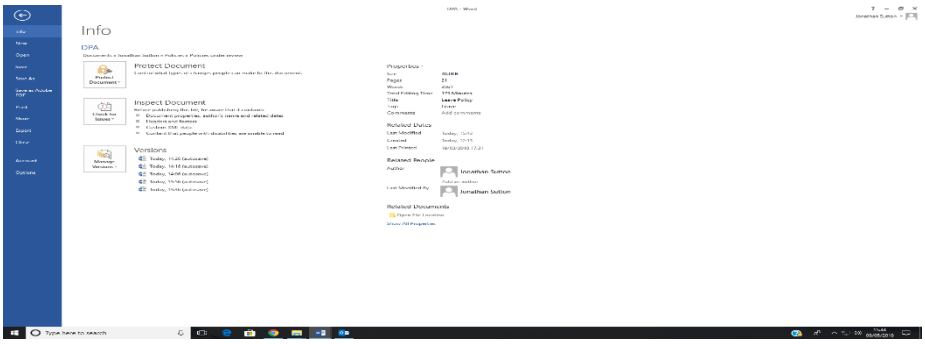
[1] To do this File the document (File / Protect Document) provide a strong password. The password to be communicated to the recipient(s) using another communications channel but not email (if the protected document was sent by email). For example, the password "2Xs5@97h" might be sent by text message to the recipient or given during a telephone call.

Transmission by postal or courier services

76. Documents containing personal data must be secure during postal transit. This always applies to Disclosure and Barring Information where a collection of personal documents are sent together and if lost, could compromise the individual's privacy more than they might as individual documents.

77. DBS applications, including all supporting paperwork, are always secured using the 'double envelope method'. Two envelopes are used. They are marked as follows;

a. Inner envelope, the following words are to be used (no deviation is allowed) "*If this envelope is found then it must be kept safe and secure. Please do not open it. Contact the following number 01905 723729 and report the matter to the staff on duty. You will be asked for your name, contact details, where and when you found the envelope and how our staff can collect it*".



b. The outer envelope is to contain the address of the recipient, and on the reverse, the address that the envelope is to be returned to. For example "If found, please return to Data Compliance Officer, St Paul's Hostel Tallow Hill Worcester WR5 1DB".

78. All DBS applications must be sent by Royal Mail Signed For Second Class.

79. Passing personal data to Third Parties. There is often a need to pass information from CCTV to the Police. This must be undertaken only by the DPO, or if absent, someone who has been delegated. These restrictions are necessary because USB ports in most computers are disabled.

80. Any USB or CD containing information must be carefully accounted for and signed for. The form in this policy must be used.

81. Disposal of equipment. The disposal of equipment carries a risk of data breach. In no circumstances is any IT equipment, or parts of, that hold data to be disposed of in the public waste service. They are to be disposed of by our IT provider. The Form in this policy is to be used.

THE PROCEDURE FOR RESPONDING TO SUBJECT ACCESS REQUESTS

Background and context

82. Individuals benefit from heightened rights in terms of their ability to request and access personal data from any entities holding such data about them. Other rights, however, are novel or enhanced to react to the developments in the digital age. For example, if an individual makes their request electronically, an organisation should provide the information in an electronic format. Furthermore, the GDPR introduces a best practice recommendation that where possible organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to their information.

Fees

83. In most cases St Paul's will no longer be able to charge the individual for the administrative costs of finding, gathering and disclosing data to the individual unless the individual's request is "*manifestly unfounded or excessive*" (which is expected to be a high threshold to satisfy). An example of a scenario where a fee could be charged is if a request is repetitive or if additional copies of the data are requested. However, if the Subject Access Request is either unfounded, excessive or repetitive an Organisation may be able to charge for dealing with the request by levying a "reasonable fee" (which is not defined) to take into account the administrative costs of providing the information.

Timing

84. Information must be provided to the individual without delay, and at the latest, within (30 days) one month of receipt of the request.

85. An extension of this deadline by a further two months where the individual's requests are complex or numerous. In these cases, the individual must be notified of this within a month of receipt of the request, providing its reasons for the delay.

Unfounded and excessive requests

86. In addition to being able to charge the individual if their request is unfounded and/or excessive (for example if there is repetition in the request), organisations may outright refuse to respond to the request. If they choose to do this, however, reasons for the refusal must be given to the individual. The individual will also need to be informed of their right to complain to the relevant supervisory authority (which will be the Information Commissioners Office) and of their right to a judicial remedy. Both the reasons for refusal and the advising of the right to complain should be put to the individual without undue delay and, at the very latest, within one month of the request.

What counts as a valid Subject Access Request

87. In order for a subject access request to be valid it must be made in writing. However as this includes various digital and physical formats it is important to understand what does or does not count as valid.

88. It is possible for an individual to make a subject access request on social channels, such as Twitter or Facebook or via email. You must treat these applications as valid and respond to the individual within the 30 day timescale.

89. A request sent via fax is considered to be a valid hard copy.

90. If a written request fails to mention that it is a subject access request, but it is clear that the individual is asking for their own personal data, it is still valid and should be treated as such.

91. Similarly, a Subject Access Request is considered valid, even when it has not been sent to a person in your company who usually deals with this kind of request.

92. A verbal request is not considered valid in most cases. However, good practice suggests you at least offer the individual information about how to make a subject access request

93. As with any request of this nature, there are always exemptions to what is considered valid. For example, if a disabled person is unable to make a subject request in writing, you may have to make adjustment for them under the Equality Act 2010 (Disability Discrimination Act 1995 - Northern Ireland). You may also have to make a similar provision to the format: Braille, audio transcribed, large print etc. Failure to make provision may not put you at risk of GDPR non-compliance, but will certainly put at risk of a claim under the Equality Act.

What information should a subject access request contain?

94. A subject access request details:
    a. How and to what purpose personal data is processed
    b. The period you intend to process it for
    c. Anyone who has access to the personal data
    d. The logic involved in any automatic personal data processing

95. We have the right to withhold information that would compromise or reveal:
    a. The personal data of another individual
    b. Intellectual property
    c. Trade secrets.

96. There may be times when responding to a Subject Access Request would mean disclosing the personal information of another person. In most cases, as mentioned above, you do not need to include this information except where:

a. The other individual has consented to the disclosure; or

b. It is reasonable in all circumstances to comply with the request without that individual's consent.

97. The GDPR regulations recognise that while completing a Right of Access is fundamental, organisations should not be expected to provide information simply because an individual is interested in it. Unless they are acting on behalf of another person, an individual is only entitled to see their own personal data.

98. The DCO must establish whether the information requested falls under the definition of 'personal data'. If it does not, you are not obligated to respond to the Subject Access Request. The DCO must also keep in mind that this does not exempt from providing *any* information to the individual making a Subject Access Request. We are obligated to provide as much information as possible when an individual makes a subject access request. Which is why it is important to understand exactly what information your company holds as well as developing a clear data management strategy.

What format do we respond in?

99. We will provide a copy of the information to the individual in an easy to access format. GDPR guidelines state that '*the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.' If the* individual makes the request digitally, the response must be provided in a commonly used digital format.

How do I make sure I have located all the data necessary for a Subject Access Request?

PROCEDURE FOR DEALING WITH A SUBJECT ACCESS REQUEST

100. The procedure is;

a. Notify the Data Protection Officer (DPO) as soon as possible. Do not wait longer than 48 hours to notify because the timescale to reply to a SAR is 30 days.

b. The DPO is to set up a new file with the name of the SAR.

c. The DPO will then undertake an electronic and physical search of all electronic and paper files. These will be collated and where necessary the personal data of third parties will be redacted.

d. An inventory of the data will be created.

e. A reply provided to the subject, by the means stipulated in the SAR.

PROCEDURE FOR NOTIFICATION OF DATA SECURITY BREACHES TO THE INFORMATION COMMISSIONER'S OFFICE (ICO)

Background and context: What the Data Protection Act says

101. It is not the case that all personal data breaches will need to be reported to the ICO. Under GDPR it is mandatory to report a personal data breach to the ICO if it's likely to result in a risk to people's rights and freedoms. Therefore the key part of whether or not to report a breach is to determine the likelihood of a risk to people's rights and freedoms from the breach.

What is a personal data breach?

102. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

103. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

What breaches do we need to notify the ICO about?

104. When a personal data breach has occurred, the DCO will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then the ICO must be notified. If is unlikely then the ICO does not need to be notified. However, not deciding to notify the ICO of the breach requires justification and this will need to be documented.

105. In assessing risk to rights and freedoms, the DCO will focus on the potential negative consequences for individuals*. Recital 85 of the GDPR explains that: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control of their personal data limitation of their rights, discrimination, identify theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality or personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned"*

106. This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data

breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. All events need to be assessed on a case-by-case basis looking at all relevant factors.

Internal procedures for dealing with a potential or actual personal data breach

107. The internal procedure follows a four-step process:

a. Step 1: The discovery of a loss or suspicion of a breach

b. Step 2: The decision whether to report the breach to the ICO

c. Step 3: Identification of what went wrong?

d. Step 4: What needs improving to prevent a reoccurrence?

TEMPLATE TO BE USED FOR DECISION TO NOTIFY (OR NOT) THE ICO

Step 1	**Discovery of a loss or suspicion of a potential loss of Personal Data** **If you are very sure or certain there has been a data breach then write down details using the headings below. Give details of**; 1. Describe what happened. 2. Describe how the incident occurred. 3. How did we discover the breach? 4. What preventative measures were in place? 5. Was the breach caused by a cyber incident (Yes or No)? 6. When did the breach happen (Date and time)? 7. When did we discover the breach? (Date and time)? 8. What categories of personal data in the breach? 9. How many personal data records are included in the breach? 10. Number of Data Subjects affected? 11. Categories of Data Subjects (Employees, volunteers, residents)?	**Guidance**: **Check you dealing with a personal data breach?** A personal data breach will have occurred whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. **Action:** Notify the Data Compliance Officer or the Duty Manager first thing the next day, even if this is during a weekend or bank holiday. Do not wait longer than 12 hours. **Guidance**: Use the 11 questions in Step 1 to guide you. **Action**: Make a note of when you completed this task: Date Time Initials of person reporting
Step 2	**Decision by Data Compliance Manager (or Duty Manager) whether to report the matter to the ICO.** When a personal data breach has occurred, we must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then we must notify the ICO. On the other hand if it is unlikely then we do not have to report it. However, the decision not to report the report the breach must be justified and documented. In assessing risk	**Guidance**: Tell it all, tell it fast, tell the truth and always report an incident if you are not sure whether you should or not. **Guidance**: A notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

	to rights and freedoms, it's important to focus on the potential negative consequences for individuals. 1. What are the potential consequences of the breach? 2. Is the personal data breach likely to result in high risk to data subject? 3. Had the staff member involved in this breach received data protection training in the last two years? 4. (Initial reports only) If there has been a delay in reporting this breach, please explain why 5. Have you taken actions to contain the breach? Please describe these remedial actions 6. Have you told data subjects about the breach? 7. Have you told data subjects about the breach?	**Guidance**: The Data Compliance Officer should always notify the ICO unless there are exceptional reasons and another senior person has to do it. For example, if the DCO is on leave or absent from the office for an extended period. **Guidance** to make a decision. "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identify theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentially of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. **Guidance**: Consider the 7 questions and write down the answers. **Action**: Always notify Chair or Vice Chair of Trustees <u>before</u> notification to ICO if by doing so this will **not cause** undue delay. The ICO website provides contact telephone number or online form. Notifying the ICO you will need; • The data controller is St Paul's hostel • Registration number Z9152112

		Action: Notify the individuals who personal data has been breached as **soon as possible**. **Action**: Make records of your actions.
	Justify and document your decision if you decide NOT to report a breach to the ICO	
Step 3	**Identification of what went wrong** The output of this step should answer the following questions: What happened? Why? Was this a breach of policy? Was this a breach of procedure?	**Guidance:** Lessons need to be identified before they can be learnt. This step should be done meticulously but not expressing accusation or blame. **Guidance**: This step must always be led by the Data Compliance Officer with support from all staff.
Step 4	**What needs to be improved to prevent this happening again?**	**Guidance:** This step must be led by the Data Compliance Officer and involve all staff.

DATA RETENTION

1. St Paul's Hostel recognises the importance of effective record keeping and data management to enable it to operate effectively. To comply with the principles of current Data Protection legislation, records containing personal data must be:

   a. kept safe and secure
   b. kept for no longer than is absolutely necessary
   c. disposed of securely

2. Additionally, enhanced confidentiality is required for "special category" data, such as:

   a. ethnic background
   b. political opinion
   c. religious belief
   d. medical information
   e. criminal record

WHAT DOCUMENTS DOES THIS GUIDANCE APPLY TO?

3. This guidance applies to electronic data, paper records and cloud-based data. The period of retention commences when the record is closed.

GENERAL - STORAGE OF RECORDS

4. All data should be stored as securely as possible in order to avoid potential misuse, theft or loss.

5. Working documents that are not considered to be records should be securely disposed of as soon as they are no longer required.

6. Where Data and records are no longer active due to their age or subject, but need to be retained for a lawful purpose, they should be archived.

7. Any data file or record which contains personal data should be considered as confidential in nature and managed in line with the Data Protection Act 2018 (GDPR).

RETENTION SCHEDULE

8. No file should be retained for more than a maximum period of 6 years (after it is closed) unless a sound and lawful reason can be demonstrated. In most cases, the period of retention will be considerably shorter. Where it is possible to break down a file (retaining only what is necessary) this should be done. Review and delete!

9. Reasons for longer retention may include:

a. Statutory requirements (see Appendix A);

b. The record contains information relevant to legal action which has been started or is 'reasonably' anticipated (in this event, records and information that are likely to be disclosable should not be amended or disposed of until the threat of litigation has been removed);

c. Where a decision is made to retain records for a longer period, the file should be clearly annotated with the reason why and who made the decision.

DISPOSAL

10. In line with the Data Protection Act 2018, all information containing personal data (that is relating to living individuals) must be securely destroyed when it is no longer required.

11. When records or data are identified for disposal, a register of such records or data must be kept indicating the date of disposal.

12. ‘Hard copy’ records should be disposed of by shredding.

13. Electronic data should be disposed of in line with the Data Protection policy.

14. Back up copies of such data also need to be securely disposed of.

FURTHER INFORMATION

15. If you have questions or require further guidance, please speak to the Data Compliance Officer.

RETENTION SCHEDULE

STATUTORY		
Type of Data	Minimum Retention Period	Reason
Accident books, Accident records and reports	3 years from date of last entry (1)	Statutory - The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) as amended
Accounting records	6 years after the financial year to which they relate	Section 221 of the Companies Act 1995 as modified by the Companies Acts 1989 and 2006
Income Tax and NI returns, income tax records and correspondence with HMRC	3 years after the financial year to which they relate	The Income Tax (Employment) Regulations 1993 (as amended)
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of last entry	The Control of Lead at Work Regulations 1998 (as amended)
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from date of last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH)
Medical records under the Control of Asbestos at Work Regulations	40 years from date of last entry	The Control of Asbestos at Work Regulations 2002 (as amended)
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches age 75, but	The Ionising Radiations Regulations 1999

	in any event for at least 50 years	
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH)
Records relating to children and young adults	Until the child/young person reaches the age of 21	The Limitation Act 1980

Retirement Benefits Schemes - records of notifiable events, eg relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Statutory Maternity Pay records, calculations and certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	Statutory - the Statutory Maternity Pay (General) Regulations 1986 (as amended)
Statutory Sick Pay records, calculations, certificates and self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (as amended)
Wage and salary records (also overtime, bonuses, expenses)	6 years after the end of the tax year to which they relate	Taxes Management Act 1970
National Minimum Wage records	3 years after the end of the tax year to which they relate	National Minimum Wage Act 1998
Records related to Working Time	2 years after the end of the tax year to which they relate	The Working Time Regulations 1998
NON STATUTORY		
Type of Data	Minimum Retention Period	Reason
Application forms (unsuccessful candidates)	6 months	In case of complaints or discrimination claims NB Successful candidates A/Fs will be transferred to their Personal file
Equal Opportunities Form (unsuccessful candidates)	6 months	As above. These should be filed separately as they contain special category information.

Interview notes and assessment tests (panel members must hand in all paperwork at end of interview to avoid duplicate retention)	6 months	As above.
Pre-employment health screening forms and reports (rejected or withdrawn preferred candidates)	6 months	As above. These should be filed separately as they contain special category information.
Personal file, including Application form and references	6 years after employment ceases (2)	
Equal Opportunities Form (current staff)	6 years after employment ceases	These should be filed separately as they contain special category information
Pre-employment health screening form and reports (current staff) and any other medical information relating to staff	6 years after employment ceases	These should be filed separately as they contain special category information
Disciplinary records Staff disciplinary records including details of investigation, meeting notes, etc (panel members must hand in all papers at end of meeting to avoid duplicate retention)	6 years after employment ceases	Any warnings must be removed from the Personal file in line with the Disciplinary Procedure and as quoted in letter. First Written warnings - 1 year Final Written warnings - 1-2 years

Training records	6 years after employment ceases	
Risk assessments under Health and Safety Regulations	Permanently	In case of claims
Inland Revenue/HMRC approvals	Permanently	
Parental leave forms	Until the child's 18th birthday	
Redundancy details, calculations of payments	6 years from date of redundancy	
Time sheets	2 years after audit	

(1) Under the Limitation Act 1980, if the accident involves a child/young adult, records must be retained until that person reaches the age of 21

(2) Files should be broken down retaining only basic information and deleting any data which is no longer relevant.

PRIVACY NOTICES V1.0

PRIVACY NOTICE FOR EMPLOYEES AND WORKERS
in compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation ("GDPR")

1. St Paul's Hostel "the organisation" takes the security and privacy of your personal data seriously. We have internal policies and controls in place to try to ensure that your personal data is not lost, accidentally destroyed, misused or disclosed and is processed fairly, lawfully and transparently in line with our Data Protection Policy, a copy which can be obtained from the Chief Executive's office.

2. St Paul's Hostel is a 'Data Controller' for the purposes of your personal data; this means that we determine the purpose and means of the processing of your personal data.

3. As your employer, we need to gather and use information or 'data' about you as part of our business of running the charity and to manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left.

4. This includes using information to enable us to comply with the employment contract, to comply with legal requirements, pursue the legitimate interests of the employer and protect our legal position in the event of legal proceedings.

5. Much of the information we hold will have been provided by you, for example on your application form, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees or background check providers.

6. We will collect and use the following types of personal data about you:

   a. your application form (or CV), qualifications, membership of professional bodies and pre-employment assessments;
   b. information about your suitability for the post, including references and security and/or DBS checks;
   c. your contact details and date of birth;
   d. the contact details for your emergency contacts;
   e. your gender, your marital status and family details;
   f. information about your contract of employment (or services), including start and end dates, role and location;
   g. your working hours;
   h. details of promotion, salary (including salary history), pension and benefits;
   i. your holiday entitlement;
   j. your absences from work, including sickness absence;
   k. your bank details and information related to your tax status, including your national insurance number;

l. your identification documents including passport and driving licence and information in relation to your immigration status and right to work in the UK;
m. information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
n. information relating to your performance and behaviour at work;
o. training records;
p. information in relation to your use of IT systems or telephones/mobile phones belonging to the organisation;
q. your images (whether captured on CCTV, by photograph or by video);
r. information used for equal opportunities monitoring;
s. any other category of information which we may notify you of from time to time.

7. You will, of course, inevitably be referred to in many other documents and records, including e-mails, that are produced by you and your colleagues in the course of carrying out your duties and the business of the organisation.

8. Where necessary, we may keep information relating to your health, which could include reasons for absence and GP or Occupational Health reports and notes. This information will be used in order to comply with our Health and Safety and Occupational Health obligations, to consider how your health affects your ability to do your job and whether any reasonable adjustments to your job might be appropriate. We will also need this data to administer and manage sick pay in line with your contract and our legal obligations.

9. 'Special categories' of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, health, sexual orientation or any criminal convictions and offences, will only be processed in certain situations in accordance with the law. For example, we can do so if we have your explicit consent or if the information is required to protect your health in an emergency. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

10. We will use your personal data for:

a. Performing the contract of employment (or services) between us;
b. Complying with any legal obligation; or
c. Necessary to protect the vital interest. For example, if you are seriously ill we will pass your medical information to the medical staff.
d. If it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interest and request that we stop this processing.

11. We can process your personal data for these listed purposes without your knowledge or consent. However, we will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

12. The organisation shares your data with third parties in order to obtain pre-employment references from others eg former employers and DBS checks. We may share your personal data with third parties/outsourced providers to carry out our obligations under our contract with you, eg payroll provider, HR providers, pension providers, Occupational Health providers or health insurance schemes who process data on the Company's behalf or for other legitimate purposes. We require those third parties to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

13. We may also share your personal data in the event of a transfer of undertakings (TUPE); in such circumstances the data will be subject to confidentiality arrangements.

14. Further, we may share your personal data where we are legally obliged to do so, eg with HMRC or law enforcement agencies.

15. We will not transfer information about you outside of the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

16. We do not use automated decision making or profiling.

17. Your personal data will be stored in a range of different places, including in your personnel file, in the organisation's HR management system and other IT systems including the organisation's e-mail system. Information will be stored and disposed of in line with our Retention and Disposal policy and we will only hold data for as long as necessary for the purposes for which we have collected it.

18. If in the future we intend to process your personal data for a purpose other than that which it was collected, we will provide you with information on that purpose and any other relevant information.

YOUR RIGHTS UNDER GDPR AND THE DATA PROTECTION ACT 2018

19. As a data subject, you have a number of rights. You can:

a. Access and obtain a copy of your data on request;

b. Require the organisation to correct incorrect or incomplete data;

c. Require the organisation to erase or stop processing your data, for example where the data is no longer necessary for the purposes of processing;

d. Object to the processing of your data where the organisation is relying on its legitimate interests as the legal grounds for processing; and

e. Ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

20. St Paul's Hostel's nominated Data Compliance Officer is the Chief Executive who should be advised, in writing or orally, if you have any concerns regarding the processing of your personal data or would like to exercise any of these rights.

21. In addition, you have the right to lodge a complaint to the Information Commissioners' Office (ICO) if you believe that we have not complied with the requirements of the GDPR or DPA 2018 with regard to your personal data.

WHAT IF YOU DO NOT PROVIDE YOUR PERSONAL DATA?

22. As an employee, you have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith.

23. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements, eg maternity/paternity/shared parental leave. Failing to provide the data may mean that you are unable to exercise your statutory rights.

24. Certain information, such as contract details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you and to fulfil our legal obligations, eg to HMRC.

25. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Signed on behalf of the employer:	
Position:	J E SUTTON
Date:	15 May 2018

I acknowledge and confirm receipt of the Privacy policy

Signed by the employee or worker:	
PRINT NAME:	
Date:	

PRIVACY NOTICE FOR RESIDENTS V1.0
(Short version)
in compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation ("GDPR")
Understanding the General Data Protection Regulation (GDPR)

What is GDPR?

1. The GDPR is a comprehensive data protection law that replaces existing European privacy laws and strengthens the protection of personal data in an increasingly data driven world. The GDPR is enforceable in each EU member state and gives individuals greater control over their personal data.

Why does GDPR matter?

2. The GDPR comes into effect on 25 May 2018. St Paul's are updating our processes, systems and policies now to make sure we are fully prepared.

What is personal data?

3. Any information related to a natural person (an individual) that can be used to directly or indirectly identify the person. It can be anything from a name, a photograph, an email address, bank statement, posts on social networking websites, medical information or a computer IP address.

What does it affect?

4. The GDPR applies to any organisation that processes personal data of EU individuals, regardless of whether the organisation has a physical presence in the EU. St Paul's helps people who are from the EU and we employ staff and have the help of volunteers all who live in the EU.

What do I need to do?

5. Our new Privacy Policy / Statement will go into effect from 25 May 2018. Please read it and make sure you familiarise yourself with contents.

Who to contact?
The person responsible for GDPR is available 0830 – 1700 on Monday to Friday. If you have any specific concerns around the privacy of your personal data or require further information about how we manage your personal information, please get in touch with Data Compliance Officer (CEO).
By post: St Paul's Hostel, Tallow Hill, Worcester WR5 1DB
By phone: 01905 723729
By email: admin@stpaulshostel.co.uk

PRIVACY NOTICE FOR RESIDENTS V1.0
(Long version)
in compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation ("GDPR")

1. We provide services ourselves or use the services of third parties to help us achieve our mission, which is *to help people live through homelessness*. We must be compliant with the new EU data protection laws, we have updated our Privacy Policy and internal processes.

2. These updates ensure we are complaint with the new European Laws (known as General Data Protection Regulations, or GDPR) and give you more transparency and control over how we deal with your personal information.

HOW WE COLLECT DATA

3. **As a resident** of St Paul's Hostel, including our Resettlement houses, we collect personal data about you in connection with our service in the following ways;

a. From the Service Referral Form we receive from Local Authority Housing Teams, Worcester City Council, Probation Services or other referral agencies.
b. Through your interactions with us whether over the phone, in person, in writing or through emails.
c. From the Revenue and Benefits office, Probation Services and the Police.

HOW WE USE YOUR PERSONAL DATA

4. **As a resident** the main ways in which we may use your personal information are to;

a. Help us decide which service are appropriate for you.
b. Communicate with you and provide information on third party services.
c. Administer state benefits that you may be entitled to by staying at St Paul's hostel.
d. Maintain the safety of others in our services, as well as detect and investigate activities that may be illegal or put others at risk of harm.

SHARING YOUR PERSONAL INFORMATION

5. **As a resident** we may share your personal information with third parties who provide services for us or for you such as;

a. Revenue and Benefits Offices
b. Local Authorities
c. Housing Authorities
d. Homeless Services

e. Probation services
f. Drugs and alcohol services
g. Adult Social Care
h. Children's Services
i. Police service

6. **We will do this to**:

a. Ensure you have the state benefits you are entitled
b. Refer you to other services you need
c. Safeguard you and others in our service.
d. Comply with our legal obligations; court orders, laws or regulations

HOW THE LAW PROTECTS YOU?

7. Data protection law say that we are allowed to use personal information only if we have proper reason to do so. When St Paul's processes Personal Data, whether as a Data Controller or as a Data Processor, we will rely on the following grounds for processing each of the categories of data we hold.

Residents	**Contract**. The categories of data are necessary to allow St Paul's to assess a person's suitability for our services, communicate with them and obtain the necessary Housing Benefit income for the service. Necessary to protect your **vital interest**. For example, if you are seriously ill we will pass your medical information to the medical staff. **Legal reasons**. Where required by court orders, laws or regulations. **Legitimate interest**. Our legitimate interest is the administration of the charity.

Retaining your personal information

8. We will retain your personal information for as long as is necessary for the purposes described above. Typically, we will retain your data for a minimum of seven years; to fulfil our business purposes, to comply with legal and regulatory requirements or for any legal claim.

9. We may keep your data for longer where this is necessary for statistical and historical research purposes. However, we will ensure all personally identifiable information is

removed where technically feasible. We will maintain the security and protection of any information we hold.

YOUR DATA SUBJECT RIGHTS

10. As well as our obligations and commitment to respect the privacy of your information, you also have certain right relating to the personal information we hold about you which are outlined below. None of these are absolute and are subject to various exceptions and limitations. You can exercise these rights at any time by contacting us using the details provided in this notice.

11. You have rights to;

Request access to the information we hold about you (Data Access Request)

12. You may request access to a copy of the personal information we hold about you. We can refuse to provide information where to do so may reveal another person's personal data or would otherwise negatively impact another person's rights.

Object to processing (Right to object)

13. You may object to us using your personal data for direct marketing. This includes any profiling we perform as part of our direct marketing activities. Once we receive and have processed your objection, we will stop using your personal data for these purposes.

Request a copy of your data (Data Portability)

14. Where you gave us the information directly or via the referral form sent to us, and it was processed electronically, you can request the data we hold on you in a commonly used machine-readable format.

Request that your data is deleted (Right to be forgotten)

15. You can ask us to delete the personal information we hold about you when it is no longer required for a legitimate business need, legal or regulatory obligations or for the purposes it was collected for.

Amend or correct your information (Right to rectification)

16. If you believe that the personal information we hold about you is incomplete, inaccurate or incorrect please contact us as soon as possible so we can update it.

Restrict the processing of your information (Right to restrict)

17. You may ask us to restrict our processing of your data whist we resolve any complaint you have about the way your data is used, require it for legal claim or if you think our processing is unlawful but you do not want us to delete your data.

Rights in relation to consent (Right to withdraw)

18. At any time, you may withdraw the consent you granted for your personal information to be used for direct marketing. When you withdraw your consent, it will not affect the lawfulness of any past activities we have undertaken based on the previous consent.

How we respond to your rights

19. You can exercise these rights at any time by contacting us using the details in this notice. We may need to validate your identify before we can respond to your request.

20. If we are unable to confirm your identify, or have strong reasons to believe that your request is unreasonably excessive or unfounded, we may deny it.

21. Once we have validated your identify, we aim to respond to your requests within 30 days and not later than 3 months from receipt of complex requests. We will let you know if we need additional time to complete.

22. We will let you know whether we accept, or refuse your request.

Security

23. We take all reasonable precautions to keep your personal information secure, including safeguards against unauthorised access, use, or data loss. This includes ensuring our staff, partners and any third parties who perform work on our behalf comply with security standards as part of their contractual obligations.

Making a data protection complaint

24. If you have any concerns about the use of your personal data, or the way we handle your requests relating to your rights, you can raise a complaint directly with us using the contact details in this notice.

25. If you are not satisfied with the way we handle your complaint, you are entitled to raise a complaint directly with the UK Information Commissioner's Office via the details on their website: www.ico.org.uk

PRIVACY NOTICE FOR VOLUNTEERS V1.0
in compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation ("GDPR")

1. We must be compliant with the new EU data protection laws, we have updated our Privacy Policy and internal processes.

2. These updates ensure we are complaint with the new European Laws (known as General Data Protection Regulations, or GDPR) and give you more transparency and control over how we deal with your personal information.

HOW WE COLLECT DATA

3. As a volunteer for St Paul's Hostel, we collect personal data about you in connection with our service in the following ways;

a. From the volunteer agreement form you completed.
b. Through your interactions with us whether over the phone, in person, in writing or through emails.
c. From the Disclosure and Barring Service application you complete.

HOW WE USE YOUR PERSONAL DATA

4. As a volunteer the main ways in which we may use your personal information are to:
a. Communicate with you and provide information on our services or information about events we are holding.
b. Maintain the safety of you and others in our services.

SHARING YOUR PERSONAL INFORMATION

5. As a volunteer we may share your personal information with third parties who provide services for us or for you such as;

a. The Disclosure and Barring Service.
b. Companies House (if you are a Trustee)

6. We will do this to:

a. To comply with the volunteer agreement.
b. Protect your vital interests, for example in case of a medical emergency.
c. Comply with our legal obligations, court orders, laws or regulations.

HOW THE LAW PROTECTS YOU?

7. Data protection law say that we are allowed to use personal information only if we have proper reason to do so. When St Paul's processes Personal Data, whether as a Data Controller or as a Data Processor, we will rely on the following grounds for processing each of the categories of data we hold.

Volunteers	**Contract.** The *volunteer agreement* provides the basis for the interaction between the volunteer and St Paul's. Necessary to protect your **vital interest**. For example, if you are seriously ill we will pass your medical information to the medical staff. **Legal reasons**. Where required by court orders, laws or regulations.

RETAINING YOUR PERSONAL INFORMATION

8. We will retain your personal information for as long as is necessary for the purposes described above. Typically, we will retain your data for a minimum of three years to fulfil our business purposes, to comply with legal and regulatory requirements or for any legal claim.

9. We may keep your data for longer where this is necessary for statistical and historical research purposes. However, we will ensure all personally identifiable information is removed where technically feasible. We will maintain the security and protection of any information we hold.

YOUR DATA SUBJECT RIGHTS

10. As well as our obligations and commitment to respect the privacy of your information, you also have certain right relating to the personal information we hold about you which are outlined below. None of these are absolute and are subject to various exceptions and limitations. You can exercise these rights at any time by contacting us using the details provided in this notice.

11. You have rights to;

a. Request access to the information we hold about you (Subject Access Request)

b. You may request access to a copy of the personal information we hold about you. We can refuse to provide information where to do so may reveal another person's personal data or would otherwise negatively impact another person's rights.

Object to processing (Right to object)

12. You may object to us using your personal data for direct marketing. This includes any profiling we perform as part of our direct marketing activities. Once we receive and have processed your objection, we will stop using your personal data for these purposes.
13. Request a copy of your data (Data Portability)

14. Where you gave us the information directly or via the referral form sent to us, and it was processed electronically, you can request the data we hold on you in a commonly used machine-readable format.

Request that your data is deleted (Right to be forgotten)

15. You can ask us to delete the personal information we hold about you when it is no longer required for a legitimate business need, legal or regulatory obligations or for the purposes it was collected for.

Amend or correct your information (Right to rectification)

16. If you believe that the personal information we hold about you is incomplete, inaccurate or incorrect please contact us as soon as possible so we can update it.

Restrict the processing of your information (Right to restrict)

17. You may ask us to restrict our processing of your data whilst we resolve any complaint you have about the way your data is used, require it for legal claim or if you think our processing is unlawful but you do not want us to delete your data.

Rights in relation to consent (Right to withdraw)

18. At any time, you may withdraw the consent you granted for your personal information to be used for direct marketing. When you withdraw your consent, it will not affect the lawfulness of any past activities we have undertaken based on the previous consent.

How we respond to your rights

19. You can exercise these rights at any time by contacting us using the details in this notice. We may need to validate your identify before we can respond to your request.

20. If we are unable to confirm your identify, or have strong reasons to believe that your request is unreasonably excessive or unfounded, we may deny it.

21. Once we have validated your identify, we aim to respond to your requests within 30 days and not later than 3 months from receipt of complex requests. We will let you know if we need additional time to complete.

22. We will let you know whether we accept, or refuse your request.

Security

23. We take all reasonable precautions to keep your personal information secure, including safeguards against unauthorised access, use, or data loss. This includes ensuring our staff, partners and any third parties who perform work on our behalf comply with security standards as part of their contractual obligations.

Making a data protection complaint

24. If you have any concerns about the use of your personal data, or the way we handle your requests relating to your rights, you can raise a complaint directly with us using the contact details in this notice.

25. If you are not satisfied with the way we handle your complaint, you are entitled to raise a complaint directly with the UK Information Commissioner's Office via the details on their website: www.ico.org.uk

PRIVACY NOTICE FOR JOB APPLICANTS V1.0

in compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation ("GDPR") effective 25th May 2018

1. St Paul's Hostel "the organisation" takes the security and privacy of your personal data seriously. We have internal policies and controls in place to ensure that your personal data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by our employees in the proper performance of their duties.

2. St Paul's Hostel is a 'Data Controller' for the purposes of your personal data; this means that we determine the purpose and means of the processing of your personal data.

3. As part of any recruitment process, the organisation collects and processes personal information or 'data' about job applicants. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

4. We will collect and use the following types of personal data about you:

   - Your name, address, contact details, including e-mail address and telephone number(s);
   - Your National Insurance number;
   - Details of your education, qualifications, skills, training and membership of professional bodies;
   - Your experience and employment history;
   - Information about your current level of remuneration, including benefit entitlements;
   - Whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
   - Information about your entitlement to work in the UK;
   - Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

5. The organisation collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interview or other forms of assessment, including online tests.

6. The organisation will also collect personal data about you from third parties, such as references supplied by former employers, information from background check providers and information from criminal records checks (where applicable). The organisation will only seek information from such third parties once a provisional job offer has been made and will inform you that it is doing so.

7. Data will be stored in a range of different places, including in recruitment files, in HR management systems and on other IT systems, including e-mail.

8. The organisation needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

9. In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required by law to check a successful applicant's eligibility to work in the UK before employment starts.

10. The organisation has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The organisation may also need to process data from job applicants to respond to and defend against legal claims.

11. The organisation processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

12. Where the organisation processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.

13. For some roles, the organisation is obliged to seek information about criminal convictions and offences. Where the organisation seeks this information, it does so because it is necessary to carry out its obligations and exercise specific rights in relation to employment.

14. The organisation will not, without your consent, use your data for any purpose other than the recruitment exercise for which you have applied.

15. Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

16. The organisation may share your data with third parties such as external HR providers for shortlisting or other recruitment/assessment assistance.

17. If your application is successful and the organisation makes you a provisional offer of employment, your data may be shared with former employers (or other referees nominated by you) for reference purposes, employment check providers to obtain necessary background checks and the Disclosures and Barring Service to obtain necessary criminal records checks (where applicable). We require those third parties to keep your personal

data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

18. The organisation will not transfer your data outside the European Economic Area.

19. If your application is unsuccessful the organisation will hold your data on file for 6 months after the end of the relevant recruitment process.

20. If your application is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. You will be provided with a new Privacy Notice for employees and workers.

21. As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request;
- Require the organisation to correct incorrect or incomplete data;
- Require the organisation to erase or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- Object to the processing of your data where the organisation is relying on its legitimate interests as the legal grounds for processing; and
- Ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

22. If you would like to exercise any of these rights, please contact the organisation's Data Compliance Officer who is the Chief Executive.

23. In addition, if you believe the organisation has not complied with your data protection rights you can complain to the Information Commissioners' Office (ICO).

What if you do not provide personal data?

24. You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all.

25. You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Automated decision-making

26. The organisation’s recruitment processes do not rely on automated decision-making.

DATA TRANSFER RECEIPT

1. Security of data in transit is a possible risk where data is lost. This form is to be used where data (for example CCTV footage) is transferred from one Data Controller to another. St Paul's is a data controller.

2. The following data has been transferred.

    a. The organisation receiving the data (who are a data controller) For example West Mercia Police. PC Billy Bragg (and collar number such as PC 123465)
    b. Name of data subject. S BLOGGS
    c. The medium for transfer (CD, USB) **USB stick**
    d. Number of files;
        i. One MP4 1,595 KB onto West Mercia Police WOR 4 USB

3. List each file containing data

NAME OF PERSON RECEIVING DATA: PC Billy Bragg (and collar number such as PC 123465)

DATA CONTROLLING ORGANISATION
WEST MERCIA POLICE

DATE AND TIME OF RECEIPT

J E SUTTON
DATA COMPLIANCE OFFICER
ST PAUL'S HOSTEL

**** A SIGNED COPY OF THIS RECEIPT IS TO BE SCANNED AND KEPT ON FILE. WHERE CCTV DATA IS TRANSFERRED A COPY OF THE RECEIPT IS KEPT ON THE KEY WORK NOTES ON THE DATA SUBJECT**

DISPOSAL OF EQUIPMENT RECEIPT

The following item(s) are to be disposed of. The receiving organisation will make sure all data is removed before disposal or they are destroyed in a manner to render the data unreadable.

Item	Serial Number	Remarks
Samsung Laptop model Superbo	GM1234-3434	*Associated items*

Name of receiving organisation
Name of person taking ownership

Name of St Paul's Hostel employee

Date and time of transfer