Brighton and Hove Speak Out

Data Protection and Data Retention Policy

Last updated August 2019

Next annual staff review August 2020

Next Trustee review – August 2022

Definitions
GDPR means the General Data Protection Regulation.
Responsible Person means Sarah Pickard

1. Data protection principles
Brighton and Hove Speak Out (Speak Out) is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by the Charity including both computerised and structured manual records from which a living individual (the 'Data subject') can be identified. This applies to all paper filing systems in which information on employees, trustees, services users, volunteers and enquirers can be accessed, as well as to computerised data held on such individuals. Personal data covers both facts and opinions about the individual and can be any type of material including text, photographs, video or audio material.

b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. Brighton and Hove Speak out is exempt from registering with the Information Commissioner's Office as an organisation that processes personal data and from having a Data Protection Officer

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Data Inventory
b. The Data inventory shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by Speak Out is processed on the lawful basis of consent (see ICO guidance for more information).
b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Speak Out's database.

TUPE: In the event of a loss of an existing contract or a new contract bid is successful, the terms of the contract may stipulate that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (commonly known as TUPE) apply. In this situation, Speak Out would be obliged to share/receive specific data about workers under these terms.

Transfer of Client Data: Whether TUPE regulations are in place or not, Speak Out must work with the organisation involved in a transfer of client data, to gain consent from service users before

that data is shared with or received from them. Services users will receive written notice that a change is taking place and that they have the right to refuse their data being transferred.

Revealing data to third parties: Data must not be revealed to a third party without the data subject's consent. This would only be breached in line with the levels of breach contained in the Confidentiality and Safeguarding Policies or in issues relating to national security.

Photo and film use: Where possible Speak Out will use consent forms for the person to sign. Speak Out will endeavour to make sure the person understands what they are consenting to and what the possible consequences may be.

Speak Out will ask each person directly for their consent before any case studies, photos or video footage they feature in is used for publicity, including any information on Speak Out's website (See Consent forms - Appendix 2)

5. Data minimisation

a. Speak Out shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. Speak Out only holds necessary information on the database. Special Category information (Equal Opportunities info) is only held if particular consent is given by pwld, volunteers or staff and is used to monitor equality issues. All staff and volunteers have received training on record keeping (Case Management and Record Keeping Guidelines) and any information embedded in the database is anonymised to enable ease of deletion when necessary.

6. Accuracy

a. Speak Out shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. Speak Out staff and volunteers are responsible for:

- Collecting accurate information on beneficiaries, volunteers and other users of Speak Out.
  - Inputting data into the organisation secure data base and keeping the record accurate and up to date.
  - Informing Speak Out of any changes to information, which they have provided, i.e. change of address.
  - Checking that any information that they provide to Speak Out in connection with their employment/volunteering is accurate and up to date.
  - Informing Speak Out of any errors or changes to their information.

Speak Out Managers and Volunteer Coordinator are responsible for:

- Ensuring that all staff and volunteers have a suitable induction training that covers the Data Protection policy, record keeping and file management.

7. Data retention

To ensure that personal data is kept for no longer than necessary, Speak Out has put in place an data retention schedule for each area in which personal data is processed and reviewed annually. (see Appendix 1)

An audit of current data, both manual and electronic must take place annually by all staff during admin week (normally in May) and will be overseen by the Responsible Person to monitor it's compliance. This will involve checking whether the data should still be kept under the retention periods (stated in Appendix 1). When data is due to be destroyed after it has reached the end of its retention period, this should be done so that the document cannot be used again (ie. files are shredded, computer files and database entries are deleted).

All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances

Under normal circumstances, shredding will take place internally but if necessary, Speak Out will outsource shredding to a local confidential shredding service and seek certificates that the information has been shredded.

Staff must then report back to the Responsible Person to confirm this has been done for their office/project.

8. Security

a. Speak Out shall ensure that personal data is stored securely

- using modern software that is kept-up-to-date.
- In a locked cabinet, drawer or locker
- If in electronic format and stored on removable media it must be encrypted
- All personal client data shared with the council and partners via email will be via a secure communications system.

If it is necessary to download personal client data to their own personnel device (when working at home) or remotely (for example to email as an attachment when working remotely) this must be immediately and permanently deleted

b. Passwords should not be obvious (ie names of children, pets and simple patterns of letters from a computer keyboard etc). Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
  - Contain a mix of alpha and numeric, with at least one digit
  - More complex than a single word (such passwords are easier for hackers to crack).
  - Be changed every 90 days

Passwords should

- Never revealed to anyone else
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Brighton and Hove Speak Out systems.
- Do not use the same password for systems inside and outside of work.

c. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
d. When personal data is deleted this should be done safely such that the data is irrecoverable.
e. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Speak Out shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).
Staff and volunteers must immediately report the loss or possible loss of data to their line manager or another Speak Out manager (or the Volunteer Coordinator in the case of volunteers). All possible data breaches will be recorded by Speak Out.

10. Rights to Access Information

Staff, volunteers and service users of Speak Out have the legal right to access any personal data that is being kept about them either on computer or in paper files. Staff, service users and volunteers will be informed of this right. (See **Subject Access Request Procedure** for the detailed procedure)

END OF POLICY

Appendix 1

1 Employment records

1.1 Personnel records

Record	Recommended retention period	Storage format	Reference
Rejected job applicant records, including: contact details application letters or forms CVs references certificates of good conduct interview notes assessment and psychological test results	**[**Six months after applicant is notified of rejection OR [*Insert longer period if there is a clearly communicated policy to keep candidates' CVs for future reference*]**]** *Application forms should give applicants the opportunity to object to their details being retained*	Paper or electronic	ICO Employment Practices Code para 1.7 Equality Act 2010, s 123
Application records of successful candidates, including: application letters or forms copies of academic and other training received references correspondence concerning employment CVs interview notes and evaluation forms assessment and psychological test papers and results	Seven years after employment ceases	Paper or electronic	Limitation Act 1980 (LA 1980), s 5

Criminal records information: criminal records requirement assessments for a particular post criminal records information forms the Disclosure and Barring Service (DBS) check forms DBS certificates	Criminal records requirement assessments for a particular post—12 months after the assessment was last used All other information in this category—as soon as practicable after the check has been completed and the outcome recorded (ie whether satisfactory or not) unless, in exceptional circumstances, **[**the data protection officer OR [*insert job title or department*]**]** assesses that it is clearly relevant to the ongoing employment relationship [*text, eg to allow for consideration and resolution of any disputes or complaints*] in which case, six months If **[**the data protection officer OR [*insert job title or department*]**]** considers it necessary to keep the information for longer than six months, the DBS should be consulted	Paper or electronic	DBS guidance for employers: Duration of criminal record check validity ICO Employment Practices Code Nov 2011, part 1.7.4
Employment contracts, including: personnel and training records written particulars of employment changes to terms and conditions	Seven years after employment ceases, unless document executed as a deed, in which case 13 years after employment ceases	Paper or electronic	LA 1980, ss 5, 8
Directors' service	Seven years from	Paper or electronic	LA 1980, ss 5, 8

contracts and any variations	termination or expiry of the contract, unless executed as a deed, in which case 13 years from termination or expiry		Companies Act 2006, ss 227 and 228
Copies of identification documents (eg passports)	Not less than two years from date of termination of employment	Paper or electronic	Immigration (Restrictions on Employment) Order SI 2007/3290, Art 6(1)(b)
Identification documents of foreign nationals (including right to work)	Not less than two years from date of termination of employment	Paper or electronic	Immigration (Restrictions on Employment) Order SI 2007/3290, art 6(1)(b)
Records concerning a temporary worker	Seven years after employment ceases	Paper or electronic	LA 1980, s 5
Employee performance records, including: probationary period reviews review meeting and assessment interviews appraisals and evaluations promotions and demotions [[For relevant organisations only] all information relevant to an assessment of the individual's fitness and propriety under the Senior Managers and Certification (SM&CR) regime or Senior Insurance Managers regime (SIMR)]	Seven years after employment ceases [[For organisations subject to the SM&CR and SIMR only] Information regarding a relevant individual's gross misconduct must be retained indefinitely]	Paper or electronic	LA 1980, s 5
Records relating to and/or showing compliance with Working Time Regulations 1998 including: registration of work and rest periods	Two years from the date on which the record was made	Paper or electronic	Working Time Regulations 1998, SI 1998/1833, reg 9

working time opt-out forms			
Redundancy records	Seven years from date of redundancy	Paper or electronic	LA 1980, s 5
Annual leave records	Seven years after the end of each tax year	Paper or electronic	LA 1980, s 5
Parental leave records	Seven years after the end of each tax year	Paper or electronic	LA 1980, s 5
Sickness records	Seven years after the end of each tax year	Paper or electronic	LA 1980, s 5
Records of return to work meetings following sickness, maternity etc	Seven years the end of each tax year	Paper or electronic	LA 1980, s 5
Records relating to Disciplinary procedures and Grievance procedures.	Seven years after employment ceases	Paper or electronic	LA 1980, s 5

1.2 Service User records

Record	**Recommended retention Period**	**Storage Format**	**Rationale**
Service user records- 1:1 advocacy	3 years after last contact/ case file closure for people receiving 1:1 advocacy	Electronic or paper	Service users are unlikely to represent for follow up 1:1 advocacy after 2 years. If they do, they will complete a new consent process.
Service user records- group advocacy	3 years after last contact/ case file closure for people receiving group advocacy	Electronic or paper	To enable Speak Out to accurately report to funders against for projects that last up to 3 years. Most projects do not last longer than 3 years
Emails	1 year	Electronic	Any important ongoing information to be stored on the secure computer system rather than emails.

1.3 Payroll and salary records

Record	Recommended retention period	Storage format	Reference
Records for the purposes of tax returns including wage or salary records, records of overtime, bonuses and expenses	Seven years	Paper or electronic	Taxes Management Act, 1970 s 12B Finance Act 1998, Schedule 18, para 21
Pay As You Earn (PAYE) records, including: wage sheets deductions working sheets calculations of the PAYE income of employees and relevant payments to them, the deduction of tax from, or accounting for tax in respect of, such payments all documents relating to any information which an employer is required to provide to HMRC under Form P11D (benefits in kind)	Three years after the end of the tax year to which they relate	Paper or electronic	Income Tax (Pay As You Earn) Regulations 2003, SI 2003/2682, reg 97
Income tax and NI returns, income tax records and correspondence with HMRC	Three years after the end of the financial year to which they relate	Paper or electronic	Income Tax (Employments) Regulations 1993, SI 1993/744, reg 55
Records demonstrating compliance with national minimum wage requirements, including hours worked	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends	Paper or electronic	National Minimum Wage Regulations 2015, SI 2015/621, reg 59
Details of benefits in kind, income tax records (P45, P60, P58, P48 etc), annual return of	Six years (but general time limit under the TMA 1970 is reducing to four years from 1 April 2012)	Paper or electronic	Taxes Management Act 1970

taxable pay and tax paid			
Employee income tax and national insurance returns and associated HMRC correspondence	Three years from end of tax year to which they relate	Paper or electronic	Income Tax (Pay as You Earn) Regulations 2003, SI 2003/2682, reg 97
Statutory sick pay (SSP) records	Three years after the end of the tax year to which they relate	Paper or electronic	The requirement to maintain SSP records for three years after the end of the tax year to which they relate was revoked in 2014, but an employer may still be required by HMRC to produce such records as are in his possession or power which contain, or may contain, information relevant to satisfy HMRC that statutory sick pay has been and is being paid. The Statutory Sick Pay (General) Regulations 1982, SI 1982/894, reg 13(A)
Wage or salary records (including overtime, bonuses and expenses)	Seven years	Paper or electronic	Taxes Management Act 1970, s 43
Records relating to hours worked and payments made to workers	Three years	Paper or electronic	National Wage Act 1998, s 9 The National Wage Regulations 1999, reg 38
Statutory maternity, paternity and shared parental pay records, calculations, certificates or other evidence	Three years after the end of the tax year in which the period of statutory pay ends	Paper or electronic	Statutory Maternity Pay (General) Regulations 1986, SI 1986/1960, reg 26
Record	**Recommended retention period**	**Storage format**	**Reference**
Records for the purposes of tax returns including wage or salary records, records of overtime, bonuses and expenses	Seven years	Paper or electronic	Taxes Management Act, 1970 s 12B Finance Act 1998, Schedule 18, para 21

Pay As You Earn (PAYE) records, including: wage sheets deductions working sheets calculations of the PAYE income of employees and relevant payments to them, the deduction of tax from, or accounting for tax in respect of, such payments all documents relating to any information which an employer is required to provide to HMRC under Form P11D (benefits in kind)	Three years after the end of the tax year to which they relate	Paper or electronic	Income Tax (Pay As You Earn) Regulations 2003, SI 2003/2682, reg 97
Income tax and NI returns, income tax records and correspondence with HMRC	Three years after the end of the financial year to which they relate	Paper or electronic	Income Tax (Employments) Regulations 1993, SI 1993/744, reg 55
Records demonstrating compliance with national minimum wage requirements, including hours worked	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends	Paper or electronic	National Minimum Wage Regulations 2015, SI 2015/621, reg 59
Details of benefits in kind, income tax records (P45, P60, P58, P48 etc), annual return of taxable pay and tax paid	Six years (but general time limit under the TMA 1970 is reducing to four years from 1 April 2012)	Paper or electronic	Taxes Management Act 1970
Employee income tax and national insurance returns and associated HMRC correspondence	Three years from end of tax year to which they relate	Paper or electronic	Income Tax (Pay as You Earn) Regulations 2003, SI 2003/2682, reg 97
Statutory sick pay (SSP) records	Three years after the end of the tax year to which they relate	Paper or electronic	The requirement to maintain SSP records for three years after the end

			of the tax year to which they relate was revoked in 2014, but an employer may still be required by HMRC to produce such records as are in his possession or power which contain, or may contain, information relevant to satisfy HMRC that statutory sick pay has been and is being paid. The Statutory Sick Pay (General) Regulations 1982, SI 1982/894, reg 13(A)
Wage or salary records (including overtime, bonuses and expenses)	Seven years	Paper or electronic	Taxes Management Act 1970, s 43
Records relating to hours worked and payments made to workers	Three years	Paper or electronic	National Wage Act 1998, s 9 The National Wage Regulations 1999, reg 38
Statutory maternity, paternity and shared parental pay records, calculations, certificates or other evidence	Three years after the end of the tax year in which the period of statutory pay ends	Paper or electronic	Statutory Maternity Pay (General) Regulations 1986, SI 1986/1960, reg 26

2 Health and safety records

Record	Recommended retention period	Storage format	Reference
Records of reportable injuries, diseases or dangerous occurrences reportable incidents	Three years from date of the entry	Paper or electronic	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR 2013), SI

Record	Recommended retention period	Storage format	Reference
reportable diagnoses injury arising out of accident at work (including [*insert organisation's name*]'s accident book)			2013/1471, reg 12
Lists or register of employees who have been exposed to asbestos dust, including health records of each employee	40 years from the date of the last entry made in the record	Paper or electronic	Control of Asbestos Regulations 2012, SI 2012/63, reg 22(1)
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry made in the record	Paper or electronic	The Control of Lead at Work Regulations 2002 (CLAW 2002), SI 2002/2676, reg 10
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record	Paper or electronic	The Control of Substances Hazardous to Health Regulations 2002 (COSHH 2002), SI 2002/2677, reg 11
Records of monitoring of exposures to hazardous substances (where exposure monitoring is required under COSHH)	Where the record is representative of the personal exposures of identifiable employee—40 years from the date of the last entry made in the record Otherwise, five years from the date of the last entry made in the record	Paper or electronic	COSHH 2002, reg 10(5)
Records of tests and examinations of control systems and protective equipment under COSHH	Five years from the date on which the record was made	Paper or electronic	COSHH 2002, reg 9
[Medical records under the Ionising Radiations Regulations 1999**]**	**[**Until the person to whom the record relates reaches or would have reached 75 years of age, but in any event for at least 50 years from the date of last entry**]**	**[**Paper or electronic**]**	**[**Ionising Radiations Regulations 1999, SI 1999/3232, reg 24**]**