DATA PROTECTION GUIDANCE

INTRODUCTION

New data protection regulation called the General Data Protection Regulation (GDPR) comes in to force in May 2018. BHS's employees, volunteers, approved centres and British Riding Clubs have a shared responsibility to follow the new data protection rules and demonstrate how we comply with them.

When anyone gives and trusts us with their personal information, it is our responsibility to treat this information in a way that lives up to their expectations and complies with all our legal obligations.

We must treat supporters' personal information properly. A serious breach of data protection law could result in criminal prosecution and a fine of up to €20 million. It would also seriously damage our reputation.

Generally, a useful way of thinking about data protection is to treat people's personal information in the same way that you would expect your own information to be treated.

DATA PROTECTION TERMS AND DEFINITIONS

Data protection regulation applies to how we process people's personal information. The key terms that we need to understand are:

Data controller – this is an organisation that collects and decides how personal information will be used

Principles – these are the rules that we must follow when processing personal information

Processing - this is what we do with personal information. It includes how we collect, record, store, share and use personal information

Personal information – includes personal data and special category personal data

Personal data - this is information about people and held in computer systems, mobile telephones or in manual records such in paper files and note books. For example, name, address, date of birth, bank account details, interests

It also includes opinions about a person. For example, notes on how you think someone has behaved, performed or appears

Special category personal data – this is information about a person's health, religion, political opinion, trade union membership, race or ethnic origin, sexuality

A **data subject -** this is the person whose personal information is being processed. For example, a member, examination candidate, pupil

A **privacy notice** – this is how we inform people about how their personal information will be used

Information Commissioner's Office (ICO) - this is the government body responsible for enforcing data protection law in the UK

THE DATA PROTECTION RULES

Personal information must be:

	collected and processed in a fair, lawful and transparent way
	used only for the reasons it was collected
	relevant and not excessive
	kept accurate and up to date, and corrected or deleted if there are mistakes
	kept for no longer than it is needed
	kept safe to protect it from being lost, stolen or used inappropriately
	processed in accordance with people's rights

PRACTICAL GUIDANCE FOR COMPLIANCE

Personal data must be processed fairly, lawfully and in a transparent manner

- ✓ Be clear and open with people about how their personal information will be used
- ✓ include a written or verbal Privacy Notice when collecting personal information. This should describe:
  - who the data controller is. For example, the British Horse Society
  - the purpose for which the personal information will be used. For example, to enter a competition or sign up for an event
  - if the personal information will be shared with any other organisations

- ✓ Only use personal information in a way that people would reasonably expect
- ✓ Think about the impact of your processing – don't do anything that could have a negative effect on the people whose personal information you are using
- ✓ Only collect and use personal information if there is a lawful basis for doing so. One of the following conditions must apply:
  - We have the consent of the person concerned
  - It is necessary for the performance of a contract
    It is necessary to protect the vital interests of someone (when it is a matter of life and death)
  - It is necessary to meet a legal obligation
  - It is required to fulfil a public responsibility
  - The processing is within the legitimate interest of the data controller

- ✓ Obtain the explicit consent of a person if you are collecting their sensitive personal data. For example, health or medical information
- ✓ Keep a record of consent for using sensitive personal data

Personal information should be used only for specified, explicit, and legitimate purposes

- ✓ Only use personal information for the purpose that was described in the privacy notice when collecting it. For example, if the privacy notice states that the information collected will be used for a competition entry, that is all it can be used for

Personal information must be adequate, relevant and not excessive

- ✓ Collect just the right amount of information for the purpose required and described in the privacy notice – no more, no less
- ✓ If a person gives you more information that you need to know, for example in an email or phone conversation, only record the relevant information
- ✓ Data protection law does not allow for personal information to be kept because 'it might become useful'

Personal information must be accurate and up to date, with errors corrected or deleted as soon as possible

- ✓ Regularly check that the personal information you hold in computer and paper records is accurate
- ✓ At least once a year destroy or delete any records that are no longer needed
- ✓ Do not use personal information if you have doubts about its accuracy
- ✓ Remind people to notify you of any changes in their personal information
- ✓ Amend your records as soon as possible if someone informs you of a change in their information

Personal information should be kept only for as long as it is needed

- ✓ We must have a valid reason for keeping personal information
- ✓ A data controller must document how long it will keep different types of records and personal information for in a Personal Data Retention Policy and Schedule
- ✓ Follow your organisation's Personal Data Retention Policy and Schedule
- ✓ When personal information is no longer required it must be destroyed or disposed of securely, for example shredded or via a confidential waste system

Personal information must be kept safely to prevent it from being lost, damaged or stolen

- ✓ Access to personal information should be on a need to know basis

- ✓ Use a password to log in to your computer so that others cannot access the personal information you hold
- ✓ If you share a computer with other people (even family members), ensure that your documents are password protected to prevent unauthorised access
- ✓ Make sure papers or screens containing personal information are not visible to others in meetings, on trains, and even in your own home
- ✓ Lock desks and cupboards used to store personal information, and keep the keys secure
- ✓ Use Royal Mail registered post to send large volumes of paper containing personal information or sensitive personal data
- ✓ If you need to send an email containing personal information, or attach a file which includes personal information to an email, password protect the email or document, and send the password in a separate email or text message
- ✓ Double check that you have attached the correct file before sending an email
- ✓ Double check that the email is addressed to the correct recipient
- ✓ Always use the bcc field (not the cc field) when sending an email to more than one person so that the recipients' email addresses are not visible to each other - unless consent to share email addresses has previously been obtained
- ✓ Take special care when travelling with computers, laptops, tablets, smart phones and paper records containing personal information

Sharing personal information

- ✓ A person's personal information must not be shared with another person or organisation without their prior consent. This includes contact details and email addresses
- ✓ If we need to share personal information with other organisations to process information on our behalf, for example, we may use a mailing company to post information for us, this must be included in the privacy notice
- ✓ We can share someone's personal information without consent, if someone's life is at risk

Personal data breaches

Personal data breaches occur when personal information is lost, destroyed or shared without consent, or if someone accesses the personal information or passes it on without consent. This can be deliberate or by accident. It includes sending personal information to the wrong person and electronic devices such as laptops and telephones containing personal information being lost or stolen. We must act quickly if there is an issue

- ✓ Data controllers must keep a record of all personal data breaches
- ✓ Serious breaches must be reported to the ICO within 72 hours of being discovered
- ✓ If you think there may have been a data protection breach or there has been a near miss, please let the Data Protection Lead at BHS know immediately dataprotection@bhs.org.uk / 02476 840452.

DATA PROTECTION GUIDANCE

Data subject rights

The data protection regulation gives rights to people. The rights that are most relevant to us are:

- **The right to be informed** – we do this by including appropriate privacy notice information when collecting personal information
- **The right of access** – if asked we must give people a copy of their personal information which we hold
- **The right to object to direct marketing –** if asked we must stop sending people direct marketing messages
- **The right to rectification** – we must correct any inaccurate or incomplete personal information when asked
- **The right to erasure** – we must delete or remove some personal information if asked

How to respond to data subject rights

The right of access

A person has the right to view their personal information which hold.

- ✓ When asked we must provide this information within 30 days.
- ✓ The information provided must not include anyone else's personal information unless we have their consent.
- ✓ BHS has a procedure for responding to such requests.
- ✓ Assume that anything you record about a person could be seen by that person.
- ✓ Record facts and opinion that you would be able to defend if challenged
- ✓ If someone asks to see their personal information, contact the BHS Data Protection Lead dataprotection@bhs.org.uk / 02476 840452.

The right to object

People have the absolute right to prevent their personal information being processed for direct marketing purposes.

The definition of 'direct marketing' by the Information Commissioner's Office includes an organisation communicating its aims and objectives by email, e-newsletter, telephone, text message or post. This includes information about our campaigns, petitions, events and fundraising activities.

- ✓ You must only contact a person with a direct marketing message by electronic means (email, text message) if they have already opted in to receiving these communications by email and / or text message

- ✓ Every direct marketing message you send by email and text message must include an unsubscribe function so that the recipient has a choice to opt out of further communications from the group
- ✓ A person must not be contacted again if they unsubscribe or request not to receive further direct marketing messages
- ✓ If someone contacts you to say that they no longer wish to receive direct marketing messages by post or phone call, you must remove their name from or suppress it in your group mailing list
- ✓ A person must not be contacted again if they have requested not to receive further direct marketing messages

.

The right to erasure

The right to erasure is also known as 'the right to be forgotten'. People have the right to request the deletion or the removal of their personal information where there is no compelling reason for its continued processing. An example of this includes deleting an individual's email address from your mailing list if they ask you to after they have opted out of receiving updates by email.

- ✓ If you have given a person's personal information to someone else, you must contact each recipient of that information and ask them to erase the personal data in question
- ✓ If requested, you should also inform the person about the other recipients of their personal information
- ✓ If you have published personal information online, for example on social networks, forums or websites you should also erase the personal information from online platforms
- ✓ If you receive a right to erasure request and you're unsure how to handle it, please get in touch with the BHS Data Protection Lead insert dataprotection@bhs.org.uk / 02476 840452.