GDPR in the Company

What you need to know about changes to Data Protection

As a BB leader you will have access to lots of personal data and it is important that you understand what you need to do to keep it safe.

On 25th May 2018 data protection legislation changes with the introduction of GDPR. The ways in which personal data is collected, used and stored have changed enormously since the UK Data Protection Act was introduced in 1998. GDPR updates the law to reflect the way we live today, to ensure personal information is kept safe.

The purpose of GDPR is to give individuals more control over how data is used and how people are contacted.

GDPR requires all organisations to be transparent about the way they collect personal information (data), what it will be used for, how it might be shared and how long it will be kept for.

Implementing GDPR in the BB

The Boys' Brigade is taking a common sense approach to ensuring compliance with the new regulations and we have been working to update our policies and procedures over the last 12 months.

The Boys' Brigade is registered with the Information Commissioners Office (ICO) at HQ level and it is not necessary for Companies, Battalions or Districts to register separately with the ICO.

This document will assist Leaders in understanding how GDPR affects the BB Company and what needs to be done locally.

We have introduced a new **Data Protection Policy** and **Privacy (Fair Processing) Notice** which gives clear information about the way we collect, process, store and retain personal data.

You can find these policies and notices along with additional resources and support on our website at **leaders.boys-brigade.org.uk/gdpr**

What action do I need to take?

There are some practical steps BB Leaders need to take locally to ensure data held and processed locally is compliant.

Tick off the boxes below as you complete each step: ☑

☐ **Review personal data you hold** – review all personal data held at a Company level and create a list by checking:
- o all paper-based records that you might have in your meeting place or at home.
- o online storage systems (i.e. Dropbox, Google Drive)
- o computer devices/tablets/mobiles that you use
- o data storage devices/media (i.e. USB drives, CD's)

☐ **Review how you collect, process, store and retain data** – Using the 'Data Processing Table' *(see table on next page)* consider:
- o how data you currently hold meets the processing requirements set out (i.e. you may currently keep Consent Forms from previous sessions)
- o Identify any personal data which is held by the Company which is not detailed by the data processing table. For these you will be required to set out your own basis for lawful processing and document this.

☐ **Securely destroy** – Take action to securely destroy personal data that does not meet the processing requirements (i.e. securely destroy Consent Forms that relate to previous sessions).

☐ **Doing things differently** – You may have identified some things that you need to change, and you should take action to ensure that personal data is up to date, necessary and not held for longer than needed.

☐ **Ensure all Leaders are aware** – It is important that all leaders who handle or have access to personal data are aware of the data processing policies and follow these.

☐ **Review Regularly** – It is important that this is not seen as a one-off exercise, and that the processes are followed continually and that this checklist is reviewed at least annually.

Date Review completed: _____ / _____ / _____

By: _____

Date of next Review: _____ / _____ / _____

Keep this document along with any additional data processes you have identified. If you have any questions/concerns contact BB Headquarters.

We would also recommend that you read through our **Frequently Asked Questions** which will help you to understand how to apply the policies and processes in your Company setting.

What is personal data?

Personal data is any information that can be used to identify an individual:
- Name & Address
- Phone Number & Email Address
- Registration Number
- Date of birth
- Photograph

In addition, **Sensitive Personal Data** is sensitive information about things like a person's ethnicity, health and criminal record.

Looking for more information or advice visit the Information Commissioners Office (ICO) website at: i**co.org.uk**

Data lost of stolen?

If you think that you've lost personal data, it's been stolen or you've shared it in error, this is known as a data breach and legally you must report it to BB Headquarters immediately.

Reporting a Data Breach:
Contact our Data Protection Representative at BB Headquarters:
dataprotection@boys-brigade.org.uk
01442 231 681

Top Tips & Advice

- Use **BBHQ template forms** which have been designed to collect and provide the right information.
- Maximise the use of **Online Brigade Manager** (OBM).
- Keep paper-records like completed forms in a **secure place** (i.e. locked cupboard or cabinet).
- Ensure personal data is **kept up to date** (including your own).
- **Do NOT download personal data** to a USB/memory stick or other media.
- **Do NOT share personal data** outside of the organisation without consent.
- **Destroy/delete information** once no longer required & in line with retention policies.

Data Processing Table

The table below sets out the data processes which are typical in a local BB Company including the period of retention. If your BB Company has additional process not shown below these should be documented separately capturing the same fields for processing. For a full list of data processes see our Privacy Notes at **leaders.boys-brigade.org.uk/gdpr.htm**

Process	Process Description	Data Processed	Lawful basis	Reason for Process	Data Retention
Process which gathers data	*Full description of the process*	*Examples of data being collected for this process which drives the data categorisation*	*The lawful basis for processing the data*	*Demonstrate there is a justified reason to collect and process data*	*How long is data kept and the reason why data is to be retained*
Annual Consent Form	Child/Young Person's details are updated by Parent/Guardian	Name, DOB, Address, Telephone Numbers, Email Address, Health/Medical information	Legitimate Interest	Leaders need access to up to date contact details and health/medical details for young people in their care.	Completed paper forms should be retained securely for 12 months or until a new Annual Consent Form is completed by Parent/Guardian. Data inputted from the Consent Form into OBM will be retained until it is updated or the member leaves the organisation. Core personal details will be retained by BB Headquarters on OBM indefinitely for all children and young people (including name, dob, sex and dates started and left the organisation).
Special Activity Consent Form	Child/Young Person's details are updated by Parent/Guardian based on a special event or activity a young person is attending	Name, DOB, Address, Telephone Numbers, Email Address, Health/Medical information	Legitimate Interest	Leaders need parental/guardian permission for them to take part in a specific activity and also need access to up to date contact details and health/medical details for young people in their care during this specific event/activity.	Completed paper forms should be retained securely for 6 months after the event/activity has taken place. Data inputted from the Consent Form into OBM will be retained until it is updated or the member leaves the organisation. Core personal details will be retained by BB Headquarters on OBM indefinitely for all children and young people (including name, dob, sex and dates started and left the organisation).
Attendance Register	Recording a Child/Young person's attendance	Name, DOB	Legitimate Interest	Adult Leaders are required to keep a record of the attendance of children/young people and all adult leaders at all meetings and activities.	Records should be retained securely indefinitely, even after a child/young person or adult leader leaves the organisation.
External Event/ Activity Consent Form	A form required by an external event/activity provider, completed by child or young person's Parent/Guardian	Name, DOB, Address, Telephone Numbers, Email Address, Health/Medical information	Legitimate Interest	External event/activity providers may require their own consent or health form to be completed by a child or young person's Parent/Guardian in order to participate in the event/activity.	The event/activity provider should retain the form for the period of the event/activity, this should then be destroyed.
Newsletters	Sharing news and Information about membership	Name, Address, Email Address	Legitimate Interest	To keep members updated about news and information including sharing opportunities available to them as part of their membership.	Data is kept whilst the individual is a member of the organisation, and is securely destroyed once the member leaves the organisation.
Photos	Photos are taken, stored and used based on consent	Photo	Consent	Photos are taken to record and celebrate activities and events.	Photos are taken based on consent being given at the time.
Donation forms (including Gift Aid declarations)	Records of donations received by members & donors/supporters	Name, Address, Bank/Payment Details	Legal Obligation	We benefit from donations from members of the public who support our work. We hold personal data about these donors so that we can process donations and inform donors of our work.	Records are retained based on financial requirements for 7 years (after the last donation has been received)

Frequently Asked Questions

Some FAQ's to assist you in understanding what impact the introduction of GDPR will have on running a local BB Company:

Does GDPR apply to local BB Companies or can we leave everything to BBHQ?
GDPR is not something you can ignore. Local Companies have responsibility for the personal data that you collect and have access to and it is important that you follow BB policies and procedures in handling personal data (including 'sensitive' personal data).

How is The Boys' Brigade explaining to members what personal data it collects?
We have drawn up a "Privacy Notice" (Fair processing notice) which explains what data we collect, how it is used, where it may be stored and how long it is retained.

A copy of the Privacy Notice (Fair Processing Notice) together with the Data Protection Policy can be found on the BB website at:
http://leaders.boys-brigade.org.uk/dataprotection.

Is it still ok to use the existing consent forms or is there a new version I need to be using?
As consent forms are generally completed annually, it is fine to use the current form for the remainder of the BB session. A revised version will be launched in readiness for the 2018/19 session.

How long should I keep consent forms for?
The Annual Consent Forms should be kept for the current session and destroyed once the new session's form has been received, or at the beginning of the session if the young person has left the organisation. The Special Activity Consent Form should be retained for six months following the activity and then securely destroyed.

How do I store paper records such as Consent Forms?
Paper records including Consent Forms and Attendance Registers should be stored securely, which means ensuring access is restricted to only those registered BB Leaders that need access to that data. For example, the data should be kept in a locked room, cupboard or drawer only accessible to those individuals you can justify having access.

Best practice is to upload the data collected through the consent form to OBM which provides secure access to data on the move and even offline through OBM Anywhere. The paper records can then be kept securely at home or at your meeting place without the need to take them with you for every event/activity.

Where you do need to have paper-records with you during an activity, make sure that these are not left unattended at any time (they can be stored securely in an accessible location or kept with you at all times) and that all information is up-to-date.

How do I securely destroy paper records?
It is important that data is destroyed in line with the retention period, so for example paper records such as the Special Activity Consent Form should be stored securely for 6 months following the activity or event and then securely destroyed.

Destroying paper records means either shredding (using an electronic shredding device) or ripping/cutting up the document it so that it could not be put back together and read. It is NOT acceptable to discard whole documents without first destroying them.

What about deleting electronic records?
We are currently developing functionality on Online Brigade Manager (OBM) to manage the automatic deletion of data held for young people and leaders based on the retention periods outlined for these in our 'data processing' table in the Privacy (Fair processing) Notice.

So personal data held on OBM will be processed in accordance with the policies we have set out, but for electronic data held outside of OBM whether on your own computer/device or in the cloud (using systems like Dropbox or Google Docs) you will need to take steps to ensure that data held is deleted in line with retention periods outlined.

Is Online Brigade Manager (GDPR) compliant?
OBM is the Brigade's official membership management system and has been built to manage the needs of the organisation at all levels. OBM assists the organisation in being ready for GDPR by:

- giving access based on roles with individuals only being given access to data relevant to their role within the organisation.
- being hosted securely and requiring user credentials (two-factor authentication) to logon with SSL encryption.
- providing functionality that enables all levels of the organisation to streamline administration, keeping all data in one place, avoiding duplication and helping to keep data up to date.
- providing functionality to communicate with leaders, parents/carers and members.
- enabling leaders and parents/carers to view and update their personal data.
- managing the retention and deletion of personal data, reducing the need for paper-based records which pose a significant risk to data protection.

Can I still communicate with parents/carers via a WhatsApp group or Facebook page?
The answer is yes. With WhatsApp you need to contact the individuals and ask their permission to join the group. They'll then be able to leave at any time should they wish to. With Facebook/Twitter and other social media platforms the person would need to join (opt-in) to the group/profile anyway so there is no need to get consent for this. When using any social media platform please do not share any personal information.

What do I do if a parent/carer objects to us collecting, storing or processing data about their child?
The information collected on consent forms and the mandatory data collected and inputted into OBM is required as part of membership. Under the lawful basis for processing data we are justified and have a legitimate interest in collecting, processing and storing the data in the ways we have set out in our Privacy (Fair Processing) Notice.

If a parent/carer objects to personal data about their child being collected, processed or stored then they would have to withdraw their child from The Boys' Brigade.

Do we need to get written permission from parents/carers to communicate by email?
Where the communication is linked to a child or young person's membership it is acceptable to communicate with parents/carers by email without additional consent. This includes announcements about the programme you offer and opportunities as part of their membership.

OBM provides functionality which makes it easy to contact parents/carers by email or text message using methods which follow data protection principles including ensuring you are using the most up to date data and that personal data is not shared or stored inappropriately.

When using systems outside of OBM to send emails you should always make sure you blind copy (Bcc) recipients into the email so personal data isn't shared with the whole group. You will need to remember to keep your address book up to date and when a child leaves the organisation you will need to ensure you have a system in place to remove the parents email address from your address book.

Can I communicate regularly with past members (who are now adults)?
If you do this, you must obtain and record their consent. You also will need to ensure contact details are kept up to data and held securely.

The individuals consent is not required to communicate with members of the organisation as we will be using the legitimate interest reason to do this. However, if you communicate with past members or supporters you will require consent to continue to communicate. You will also need to be able to prove consent has been given.

What should I do about Gift Aid declarations?
OBM has the ability to manage Gif Aid declarations for parents/carers, removing the need for you to collect or store paper-based forms. Where you do use a paper-based Gift Aid form you are required to retain and store this form securely as part of your financial records for seven years (after the last donation has been received). After this period as with all paper records the form should be securely destroyed.

What about taking, storing and using photos?
It's all about consent and whether you have consent from a parent/carer. It is important you only take photos of children and young people for which you have consent. Equally you need consent to store and use the photo. If a parent/carer withdraws this consent then you should stop using any photos of that child or young person. Currently photo consent is obtained through the Annual and Special Activity Consent Forms.

Remember good practice in relation to safeguarding when taking, storing and using photos.

What about our Company archives?
Many Companies will have items including paper-based records and photos which are categorised as personal data in their archives. Keeping these items records and celebrates the Company's history and it is reasonable that such items are retained.

Anything which contains personal data including photos should be kept securely and consideration and sensitivity should be given in giving access or displaying this data publicly.

If you do include personal data in your archive, an individual can firstly request copies of any personal information you retain in an archive with an access request (a 'Subject Access Request' should be directed to BB Headquarters). So, you need to ensure that any personal data you have in the archive can be made available on request. Secondly an individual can object to the use of their personal data and in that situation, you may be required to remove/destroy all data relating to the individual.

What is a data breach?
A data breach is an incident or omission that results in a loss, theft, deletion, unauthorised sharing or access to personal data.

What do I do if I become aware of a data breach?
Firstly do what you can to contain the breach, preventing the breach from escalating. Legally you must then report it to BB Headquarters immediately, who will also be able to provide advice on what the next steps are.

You can contact our Data Protection Representative at BB Headquarters by phone on **01442 231 681** or by email at **dataprotection@boys-brigade.org.uk**.

Looking for more advice or information on GDPR?

The best place to find advice and information is the Information Commissioners Office (ICO) website at **ico.org.uk**

A Registered Charity in England & Wales (305969) and Scotland (SC038016).
The Boys' Brigade is a Company limited by guarantee, registered in England & Wales no. 145122.
Registered Address: Felden Lodge, Hemel Hempstead, Herts, HP3 0BL.

Ref: **GDPR in the Company 0518-01**