Bishop's Stortford and District

UPDATED VERSION 2nd May 2018

GDPR Toolkit March 2018

Don't Panic – this will help!

This toolkit accompanies a District presentation on the 14th March 2018 and contains paper copies of a number of electronic documents which are now available on the District website in the Members area – under GDPR.

Reference	Template *click on reference to take you to the page*	Page
1	Group/District Data Protection Policy.	3
2	Group/District Data Security Policy.	8
3	Group Privacy Notices for Parents.	13
4	District Privacy Notices for Explorer Scouts.	16
5	Subject Access Request Process.	21
6	Data Breach Process.	26
7	Group/District Using Images of Young People Policy. Revised May2018	34
8	Text for Group/District forms.	43
9	Group/District Audit Grid. ***THIS IS A SEPARATE EXCEL DOWNLOAD FROM THE WEBSITE***	

Original temples are on the District website here

It is hoped for consistency that we all adopt very similar documents across all Scout Groups and Units so that we can share updates and experiences and be confident of overall compliance. Feel free to adjust the templates to suit your Group.

REMEMBER: GDPR is not just about polices and procedures – it's about ***changing the culture*** of all volunteers in Scouting to be legal, compliant, safe and to provide confidence to parents and young people about the way we treat their valuable personal information.

If you don't follow this advice, you are running a **grave risk** and not only putting yourself, your Leaders, your Group and the District in danger but the whole reputation of local Scouting. The law is tightening up and the world is changing around us and we need to keep moving forward – this is not too difficult to set up and as long as you are on the compliance journey by the 25th May, it will be ok.

Don't leave it too long to be compliant as thing have a habit of going wrong when you least expect and remember that our parents and Explorers awareness of their new rights will increase and they will expect us to be on the ball – we need to be seen as a fit and proper organisation and not a micky mouse outfit that loses data!

If in doubt ask – don't listen to rumour!

Greg

DC 07889 130802 or district.team@bishops-stortford-scouting.co.uk

1

[insert name of Group]

***Note from Bishop's Stortford and District Scouting**: this policy has been drafted to make all volunteers adults in the Group/Unit aware of their obligations under the new General Data Protection Regulation (GDPR) from 25 May 2018. It provides practical guidance on volunteers responsibilities with Data protection - it is not aimed at parents or youth members. The District does not know how data is managed in the Group and this template should be a guide. The broad text is recommended and where there are [brackets] you need to insert your Group information. It is recommended you do not stray too far from the text as when the regulations change, the District will send out changes to this template. If you have questions email the District Commissioner, Greg* here.

Data Protection Policy for Volunteers in the Scout Group

Introduction

This policy applies to all volunteer adults in the [➔ *insert Group*] whatever their position, role or responsibilities, which includes Committee members, Occasional helpers and Young Leaders. This policy is about your obligations under the data protection legislation. Protecting Data is about ensuring the Group stores and uses information about identifiable people (Personal Data). It also gives people rights regarding their data.

In [➔ *insert Group*], we need to collect, store and process Personal Data about our volunteers, members, parents and those on waiting lists. We know that the correct and lawful handling of this data will maintain confidence in our Group and will ensure that we operate legally and successfully.
As a volunteer in [➔ *insert Group*] you are obliged to comply with this policy. Any breach is dangerous to you and the Group - data protection is a serious matter and if not followed, will have serious implications for Scouting and those volunteers concerned.

[➔ insert role (not name) of person responsible for the Group data Protection] is the Scout Group Data Protection Lead and is responsible for helping you to comply with this policy. All queries concerning data protection should be raised with them.

What information is impacted by this policy?

Data protection is about information about individuals. This is Personal Data which relates to a living person that can be identified either from that data, or from data and other information that is available. Information as simple as someone's name and address is Personal Data.

In order for you to undertake your role, you will need to handle and create Personal Data. Almost anything could include Personal Data. Examples of where Personal Data could be found are:

- on a computer database;
- in a file, such as a members record;
- On Line Scout Manager;
- health records; and
- email correspondence.

Some examples of documents where Personal Data might be seen include:

- photographs of adults and members;
- contact details and other personal information held about members and parents
- contact details potential members and parents who put their child on a waiting list;
- Bank details of a parent;
- information on a member's progress in the programme; and
- an opinion someone makes about a parent, member or volunteer in an email.

The above is not exhaustive and there may be many other ways that you use and create information that would use Personal Data. Volunteers must be extremely careful when dealing with Personal Data which falls into any of the categories below:

- information concerning Safeguarding matters;
- DBS information (handling identification papers and using the forms);
- information about confidential medical conditions and information about Special Needs;
- information concerning allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not it has been proved);
- banking information (for example about parents and volunteers);
- information about an individual's racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual orientation;
- genetic information;
- information relating to actual or alleged criminal activity; and
- biometric information.

These categories are referred to as **Special Category Data** in this policy and in the Group Information Security Policy. If you have any questions about the processing of this category of Personal Data please speak to [➔ *insert role (not name) of person responsible for the Group/District data Protection].*

Your obligations

The law requires you to ensure that all Personal Data is processed fairly, lawfully and transparently. "Processing" means virtually everything in relation to Personal Data, including using, disclosing, copying and storing Personal Data. We have to by law tell people what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious.

People must also be given other information, such as their rights about their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is provided in a document known as a "Privacy Notice". Copies of the [➔ *insert Group*] Privacy Notices for Parents can be obtained from the [➔ *insert role (not name) of person responsible for the Group data Protection]* [➔or on the website]. You must familiarise yourself with this notice.

If you are using Personal Data in a way which you think someone might think is unfair please speak to [➔ *insert role (not name) of person responsible for the Group data Protection*].

You are only allowed to process Personal Data for the following purposes:

(i) ensuring that the Scouting provides a safe and secure environment;

(ii) providing the Scouting Programme and activities for members;

(iii) protecting and promoting Scouting's interests and objectives (for example fundraising);

(iv) safeguarding and promoting the welfare of our pupils; and

(v) to fulfil the expected obligations of members and parents.

If you want to do something with Personal Data that is not on this list, or is not described in the privacy notice, you must speak to *[➔ insert role (not name) of person responsible for the Group data Protection]*. This is to make sure we have a lawful reason for using the Personal Data.

Consent

We may sometimes rely on the consent of the individual to use their Personal Data e.g. use of photographs. This consent must meet certain requirements and therefore you should speak to *[➔ insert role (not name) of person responsible for the Group data Protection]* if you think you may need to obtain consent for something, apart from those things in PO&R such as camping, swimming etc.

Limitations on data use

You must only process Personal Data for limited purposes and in an appropriate way e.g. if young people are told they will be photographed for the newspaper, you should not use those photographs for another purpose (e.g. the website). Personal Data held must be adequate and relevant for the purpose e.g. when collecting subscription arrears, you must make sure you are using all of the relevant information you have about the young person's and the family.

You must not hold excessive or unnecessary Personal Data e.g. you should only collect information about a member's siblings if that Personal Data has some relevance.

Accuracy of data

The Personal Data that you hold must be accurate – you must ensure that Personal Data is complete and kept up to date e.g. if a parent notifies you that their contact details have changed, you should update your records and those of others in the Group.

Time limits

You must not keep Personal Data longer than necessary. The [➔ *Scout Group*] has guidance about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be very careful when you are deleting data to ensure no one else can ever see it.

Keep it secure

You must keep Personal Data secure and you must comply with the following policies and guidance relating to the handling of Personal Data in the Group:

ii. Scout Group information security policy; and
iii. Policy on the use of photographs and videos of pupils.

You must not transfer Personal Data outside the EEA without adequate protection. If you need to transfer personal data outside the EEA for example an Jamboree in the USA please contact [➔ *insert role (not name) of person responsible for the Group data Protection].*

Sharing Personal Data outside of Scouting

- **You can** share Personal Data on a need to know basis - think about why it is necessary to share data outside of Scouting - if in doubt, ask the Group Scout Leader.
- **You must** encrypt emails and attachment which contain any Scouting Personal Data.
- **You must** be aware of "phishing". Phishing is a way of making something e.g. an email or a letter appear as if it has come from someone you trust. This method is used by fraudulent people to access key personal details, such as usernames and passwords. Never reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise.

- **You must not** disclose Personal Data to the Police without permission from either the District Commissioner or the Deputy District Commissioner (unless it is an emergency).
- **You must not** disclose Personal Data to third parties such as travel agents without permission from[➔ *insert role (not name) of person responsible for the Group/District data Protection*].

Sharing Personal Data within Scouting

You must only share Personal Data within Scouting on a "need to know" basis e.g. never casually chat about personal information about a child or volunteer. Examples of sharing which are **likely** to comply with the law:

- a Leader discussing a Cubs progress with the Scout Leader (for example, to ask for advice on how best to support them);
- informing the District team for an event that a Scout suffers from claustrophobia; and
- disclosing details of a Leaders allergy to wasp stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

Some examples of sharing which are **unlikely** to comply with the law:

- the District Commissioner being given access to all records kept Leaders (seniority does not necessarily mean a right of access);
- informing all Leaders in the Scout Group that a Cub has been diagnosed with autism (rather than just informing those adults who need to know and support the Cub); and
- disclosing personal contact details for an Assistant Leader (e.g. their home address and telephone number) to other Leaders (unless the Assistant Leader has given permission or it is an emergency).

You are allowed to share Personal Data to avoid harm, for example in safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues.

Individuals' rights concerning their Personal Data

People have key rights concerning their personal information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to [➔ *insert role (not name) of person responsible for the Group data Protection]*. Please also let them know immediately if anyone:

- wants to know what information Scouting holds about them or their child;
- wants Scouting to delete any information;
- asks to withdraw any formal consent that they have given to use their information or information about their child such as use of images;
- asks Scouting to correct or change information e.g. bank details, health record (unless this is a routine updating of information such as contact details);
- asks for electronic information which they provided to Scouting to be transferred back to them or to another Scout Group;
- wants Scouting to stop using their information for promotional purposes. For example, this could mean for data protection purposes communications such as a Group newsletter; or
- objects to Scouting is using their information or wants you to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

Requests for Personal Data (Subject Access Requests)

A common exercised right mentioned above is the right to make a subject access request. Under this right people are entitled to request copies of the Personal Data which the Group holds about them or in their child if under 13.

Subject access requests are often not called as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. You must always let *[➔ insert role (not name) of person responsible for the Group data Protection*] know immediately when you receive any such requests because we are required to act within a strict timeframe as set out by law.

Receiving a subject access request is a very serious matter and involves complex legal rights. You must never respond to a subject access request yourself unless the GSL authorises it.

When a subject access request is made, Scouting must disclose all of that person's Personal Data to them - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request.

Breach of this policy

Any volunteer who deliberately or recklessly discloses Personal Data held by Scouting without proper authority is guilty of a criminal offence and gross misconduct and would be subject to the consequences of the rules of the organisation. Treat Data Protection as you would Safeguarding matters – confidentially, carefully and most seriously.

Date policy AGREED:
Next REVIEW date:

2

[insert name of Group]

Note from Bishop's Stortford and District Scouting: this policy has been drafted to make all volunteers adults in the Group or Section aware of their obligations under the new General Data Protection Regulation (GDPR) from 25 May 2018. This provides practical guidance for volunteers to keep personal data safe - it is not a document for parents or youth members. The District does not know how data is looked after in the Group and this template should be a guide. The broad text is recommended and where there are [brackets] you need to insert your relevant Group information. It is recommended you do not stray too far from the text as when the regulations change, the District will send out changes to this template. If you have questions email the District Commissioner, Greg here.

Data Security Policy for Group Volunteers

1. Introduction

1.2 Information security is about what you and the Scout Group should do to make sure that all **personal data i**s kept safe and it is very important that you get this right. Most data protection fines result from information security breaches.

1.3 This Group policy need to be read alongside the Scout Group's **Data Protection Policy for Volunteers** which gives you an overview of you and the Group's obligations for data protection. You also need to read and understand the Group's Privacy Notices for Parents [➔ *insert any other polices of the Group that should be read e.g. use of images]*.

1.4 This policy is for all volunteers and Young Leaders (which includes Group Executive Members and Occasional Helpers) when handling Personal Data. If you have any questions or concerns about your obligations with this policy they should be referred to [➔ *insert role (not name) of person responsible for the Group data Protection*].

2 Be cautious!

2.1 Data security breaches can happen in different ways. Examples of breaches which get media coverage include:

- Personal Data taken after a website was hacked;
- an unencrypted laptop being stolen after being left in a car;
- sending a confidential emails to the wrong recipient;
- leaving confidential documents on a doorstep; and
- using carbon copy (cc) rather than blind carbon copy (bcc) to send emails to multiple recipients.

2.2 These give you a good idea of the type of things that can go wrong. Try and think about what problems might arise in your Section and what you can do to manage the risks. Talk to your Section Leader or Group Scout Leader if you have ideas about improving practices in the Group or Section.

2.3 You must **immediately** report all security breaches, incidents and weaknesses to the Group Scout Leader or *[➔ insert role (not name) of person responsible for the Group data Protection].*

2.4 You must **immediately** tell *[➔ insert role (not name) of person responsible for the Group data Protection]* if you see anything which might mean that there has been a security breach. You must give all of the information you can.

2.5 If it is outside normal meeting times then please report it - do not wait - report immediately no matter what time of day. All of the following are examples of a security breach:

- you accidently send an email with personal data to the wrong recipient;
- you cannot find papers which contain Personal Data; or
- any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

2.6 In certain situations the Scout Group must report information security breaches to the Information Commissioner's Office (the data protection regulator). You may also have to let those know whose information has been compromised, all within strict timescales. This is another reason why it is vital that you report breaches **immediately**.

3 Always focus on privacy

3.1 We should be thinking about data protection and privacy whenever handling any Personal Data. From May 2018, we are required to carry out an assessment of the privacy implications of using Personal Data. These assessments must be help the Scout Group to demonstrate the measures needed to prevent information security breaches from taking place, especially if we are ever involved in an investigation by the Information Commissioner's Office.

4 Special Category Data

4.1 Data protection is about protecting information about individuals. Something as simple as a person's name or their hobbies count as their Personal Data. However, some Personal Data is so sensitive that we need to be extra careful. This is called **Special Category Data** - you must be extra careful when handling **this. Special Category** Data is:

- information concerning safeguarding matters;
- information about serious medical conditions and information about Special Needs;
- information about allegations made against someone (whether or not the allegation is a criminal offence and whether it has been proved);
- bank details (for example about parents and volunteers);
- information about an individual's ethnic or racial origin;
- political views;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- genetic information;
- sexual orientation;
- information relating to actual or alleged criminal activity; and
- biometric information.

5 Limit the amount of Personal Data held

5.1 Try to keep a minimum amount of Personal Data on young people and adults helps keep data safe.

6 Using IT and computers

6.1 Many data protection breaches occur as a result of basic mistakes when using computers. Here are some suggestions to avoid problems:

- **Lock device screens:** Your phone, computer or tablet should be locked when not in use, even if you are away only for a short time.
- **Private cloud storage:** You should avoid using private cloud storage or private file sharing accounts to store or share Scouting documents. Documents should be kept in Group cloud accounts such as Google docs or a Scout Dropbox account.
- **Portable media:** Portable media devices (such as USB drives, portable hard drives, DVDs) should be kept to a minimum – avoid it if possible. If you have to use one it must be encrypted.
- **Disposal of equipment:** Laptops, printers, phones, and DVDs must always be disposed of in a secure way so that data cannot be retrieved. Seek advice on how to do this safely,

7 Passwords

7.1 Your password should be difficult to guess and must be long, for example, you could use a song lyric or a memorable phrase e.g. *standbyyourman(1966)* Your password should not be disclosed to anyone else. You could also base your password on something memorable that no-one else would know. For example the name of your first pet and your dad's year of birth. You should not use information which other people might know or be able to find out such as your address or your birthday. Passwords should not be written down.

8 Emails

8.1 When sending emails, take care to make sure that the recipients are correct.

8.2 **Emails to multiple recipients:** A blind carbon copy (**bcc**) function must be used when sending emails to multiple email recipients (more than 2) so that names and email address are not visible to other recipients. This includes email to parents, Leaders and young people. People may not want their email address seen by others and by letting other people know you would be in breach of regulations.

8.3 If the email contains Special Category Data, get someone to double check that you have entered the email address correctly before pressing send.

8.4 **Encryption:** Emails containing Special Category Data must be encrypted. For example, encryption should be used when sending details of a complaint or health matter. If you need help encrypting a file please ask *[➔ insert role (not name) of person responsible for the Group data Protection]*. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means e.g. after emailing the encrypted documents you could call the recipient with the password.

8.5 [➔ *the following point is strongly recommended*]**Private email addresses:** You must not use a private email address for Scouting related work. You must only use an email address provided to you from the Scout Group. This is because if you leave or were ill, the GSL could gain access to the information. To comply with the law, we also need access to all emails and related documents if a Subject Access Request is made. If this information is held in a private account - Scouting does not have legal control of the data.

9 Paper files

9.1 These are as important to protect as digital data.

9.2 **Keep under lock and key:** You must ensure that any papers containing Personal Data are kept under lock and key in a secure location at home or at the meeting place and that they are never left unattended.

9.3 **Disposal:** Personal Data should **never** be placed in the general waste. Paper records containing Personal Data should be disposed of by securely shredding. If you don't have a shredder as the GSL where you can use one.

9.4 **Printing:** When printing documents at the meeting place or perhaps at work, make sure that you collect everything from the printer immediately, otherwise there is a risk that confidential information could be read or collated by someone else.

9.5 **Post:** You also need to be extra careful when sending items in the post. Confidential materials should be sent by registered post and it must be marked "Private and Confidential" and contain a return to sender address

10 Keeping data at home or away from home

10.1 You might need to take Personal Data out of your home or Scout HQ site for various reasons. This does not breach data protection law as long as safeguards are in place to protect Personal Data.

10.2 **Take the minimum:** A leader organising a hike might need to take with them information about Scouts medical conditions (for example allergies and medication). If only eight out twenty Scouts are attending the trip, then the Leader should only take the medical information about the eight Scouts.

10.3 **Data on the move:** You should not work on documents containing any Personal Data whilst travelling if there is a risk of unauthorised disclosure. For example, if working on a laptop on a train, you should ensure that no one else can see the screen. Never leave any device unattended.

10.4 **Paper records:** If you need to take hard copy (i.e. paper) records out with you then you should make sure that they are kept secure. For example:

- documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);
- if travelling by car, you must keep the documents out of sight. Possessions left on car seats are vulnerable to theft;
- if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should take them with you and keep them on your person in a locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plain sight.

10.5 **Public Wi-Fi:** Public Wi-Fi is not secure so try not to use it for Scouting data.

11 Your personal devices and Scouting

11.1 You may use your personal device (such as your laptop or smartphone) for Scouting but this must be secure and encrypted.

11.2 **Security: appropriate security measures** should always be taken. Use firewalls and anti-virus software and should be kept up to date.

11.3 **Friends and family:** You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything Scouting related e.g. you should not share the login details with others and you should log out of a Scout account once you have finished. You must also make sure that your devices are not configured in a way that would allow someone else access to Scouting related documents and information.

11.4 Breach of this policy

11.5 Any volunteer who deliberately or recklessly discloses Personal Data held by Scouting without proper authority is guilty of a criminal offence and gross misconduct and would be subject to the consequences of the rules of the organisation. Treat Data Protection as you would Safeguarding matters – confidentially, carefully and most seriously.

Date policy AGREED:
Next REVIEW date:

Data Security Policy for Group Volunteers

I confirm that I have read and understood the contents of the Group Data Security Policy:

Name of volunteer:
Signed
Date

3

[insert name of Group]

Note from Bishop's Stortford and District Scouting: this Privacy Notice has been drafted to inform Parents how Scouting records, stores and handles their data under the new General Data Protection Regulation (GDPR) from 25 May 2018. This document provides practical guidance for Groups. The District does not know how data is handled in the Group at present and this template should be a guide. The broad text is recommended and where there are [brackets] you need to insert your relevant Group information. It is recommended you do not stray too far from the text as when the regulations change, the District will send out changes to this template. If you have questions email the District Commissioner, Greg here.

Privacy Notice for Parents

How we use your information

Introduction

This Privacy notice helps you understand why and how we collect your personal information and what we do with it. It also outlines decisions you can make about your own information. If you have any questions about this notice please contact to [➔ *insert role (not name) of person responsible for the Group data Protection*]

What is personal information?

Personal information is information that identifies you as an individual. Included in this is your contact details and bank details.

How and why do we collect and use personal information?

We set out below some examples of the differing ways we use personal information and where it comes from. Our main reason for using your personal information is to provide a Scouting Programme to your child.

- We obtain information about you from admissions forms and any other Scout Group your child may have been in.
- We may need to enter your details onto an on line records system such as *On Line Scout Manager*.
- We may have information about any family issues that might affect your child's happiness.
- We may take videos or photos of you and your child at events to use on social media, on our website or in other promotional communications. This helps prospective parents and young people see what we do and to help promote Scouting. We may continue to use these images after your child has left the Group.
- We may use your information in the unlikely circumstance you make a complaint about the Group.
- We may send you information about what is happening in the Group e.g. details of events and activities (including fundraising events) and newsletters.
- We may use information about you if we need this for archival purposes or for statistical purposes.
- We may also pass your details onto the Scout District if your child becomes and Explorer Scout.

Bank details

- We need your bank details so we can process membership and activities fees.

Third party information sharing

- We may need to share information in an emergency e.g. if you or your child was hurt whilst on a Scouting activity.
- We sometimes use companies to handle personal information such as *On Line Scout Manager* to help us with programme planning and communications.
- We may have to share information with local authorities, e.g. if there was a safeguarding concern.
- We may need to share some information with Scout insurance e.g. if there was an incident in the meeting place or at camp.
- We may also need to share information with the Scout, District, County or Headquarters for their advice.

Your personal data that we collect will mainly remain within Scouting and will be handled only by our volunteers on a 'need to know' basis. Any special needs data will need to be provided to Leaders more widely do we can care and support of your child.

Our legal grounds for using your information

This section contains information about the legal basis we rely upon when handling your information as outlined above.

Legitimate interests

This means we are using your information when it is necessary for our legitimate. We rely on this ground for many of the ways in which it uses your information. Specifically, the Group has a legitimate interest in:

- Providing your child with a Scouting programme.
- Managing our waiting lists.
- Improving Scouting e.g. if we want to raise money for new equipment to make sure that we are providing a good Scouting experience.
- Looking after your child and and other young people.
- Promoting what we do e.g. we may use images of your child in our materials, [our website or in our social media].

Also, your personal information may be processed for the legitimate interests of other people such as investigating a complaint. If you object to us using your information where we are relying on our legitimate interests as explained above please speak your child's Leader.

Your child's vital interests
In rare situations we may use your information to protect your child's vital interests or the vital interests of someone else (e.g. if you or they are seriously hurt).

Consent
We may ask for your consent to use your information e.g. taking photos. If we ask for your consent you can take it back at any time. Any use we have made of your information before you withdraw your consent will still remain valid.

Legal claims:
We are allowed to use your information in the case of any to legal claims – this would allow us to share details with our insurers and Headquarters.

We are required to comply with extra conditions where we handle **special categories of personal information**. These special categories include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, and information about sex life or orientation.

Sending information to other countries

We may have to send you or your child's information to countries without the same level of protection for personal information as there is in the UK e.g. a Scout event overseas. The European Commission has produced a list of countries which have good data protection regulations. Details can be found here. If the country we are sending your information to is not on the list or, is not a country within the EEA (which means the European Union, Liechtenstein, Norway and Iceland) then, it might not have the same level of security for personal information as there is in the UK. In such cases we will provide you with details about the safeguards we will put in place in this situation.

Keeping your information

We will keep your information for as long as we need to provide a Scouting programme and look after your child. We may keep some information after your child have left the Group e.g. so that we can find out what happened if you ever made a complaint.

In exceptional circumstances we may keep your information for a longer than usual, but we would only do so if we had good reasons and only if we are allowed to do so under data protection law.

We can keep your information for a long time or even indefinitely if we need it for archival records or statistical purposes. The table below shows for how long we keep different types of information.

Information type	Normal retention period
Accident and medical treatment records	Date of birth plus 25 years.
Complaints with Scouting	10 years and then reviewed.
Your child's progress record	5 Years.

What decisions can you make about your information?

Data protection legislation coming into force in May 2018 gives you rights about your information. Some of these are new whilst others build on your existing ones. Your rights are:

- you can ask for us to delete information we hold about you in certain circumstances e.g. where we no longer need the information;
- if information is incorrect you can ask for a correction;
- you can ask what information we hold about you and be provided with a copy;
- you can ask us to send you certain types of information about you in a format that can be read by computer;
- our use of information about you may be restricted sometimes e.g. if you inform us the information is inaccurate we can only use it for limited purposes while we check its accuracy.

Further information and guidance

This notice is to explain how we look after your personal information. Please ask to speak to your child's Leader if you would like us to update your information or you would prefer that certain information remains confidential. If you consider that we have not acted properly when using your personal information you can contact the Information Commissioner's Office: ico.org.uk.

Date policy AGREED:
Next REVIEW date

4

Bishop's Stortford and District Explorer Scouts

Note from Bishop's Stortford and District Scouting: *this policy has been drafted to make Explorer Scout Leader aware of their obligations under the new General Data Protection Regulation (GDPR) from 25 May 2018.*

Young People have their own rights under data protection law including the right to be informed about how their personal data is used. Parents usually exercise this right on their behalf where they are too young to understand their rights, GDPR now provides for a specific age (13 in the UK) when certain types of consent should be exercised by the young person. For pragmatic purposes, it is recommended that this consent be formalised on transfer to the Explorer Scouts by the new ES Leader

This does not apply to every type of consent e.g. a parent may consent on the child's behalf to receive medical treatment - 18 in most of the UK. There are times when a young person's consent may conflict with that of a parent – for example if the Explorer consents for their photo to be published, a parent may not want this as they have a Court order in place to stop the other parent from identifying and tacking down the child. Common sense discussions are needed in such situations.

The general principle in law is that a young person's data is their own to control, as far as their legal rights allow. A parent may be entitled to receive certain information about their child but it remains the case that for a Subject Access Request, it is the Explorer Scout who can only exercise that request provided they are mature enough to realise the consequences.

This document provides a template for the District to use.

Bishop's Stortford and District Explorer Scouts

How we use your information

Privacy Notice for Explorer Scouts

Introduction

This Privacy notice helps you understand why and how we collect your personal information and what we do with it. It also outlines decisions you can make about your own information in Scouting. We are giving you this notice because you are old enough to make decisions about your personal information. If you have any questions about this, please talk to your Leader.

What is "personal information"?

Personal information is information that identifies you as an individual. This includes information such as your name, date of birth and address as well as things like progress on awards and any medical details. We may also record your religion or beliefs or your ethnic group which we may require for the Scout headquarters annual census.

How and why do we collect and use personal information?

Our key reason for using your personal information is so we can give you a great Scouting experience.

We set out below some examples of the differing ways we use personal information and where it comes from. We get details from any Scouting admissions form, your parents and sometimes other Explorers. If you were a Scout, your Scout Leader also gave us information about you. We collect this information to help Scouting run properly, safely and to let others know what we do here. Here are some examples:

- We need to tell the Leaders and helpers if you have any health issues or are allergic to something.
- We might need to tell your Leaders if you have special needs or need extra help with some tasks.
- We may need to give some of your information to the District, County or Headquarters
- Depending on where you go when you leave us, we may need to provide your information to the Scout Network or another Explorer Scout Unit.
- If anyone makes a complaint, we may need to use your information to deal with the properly e.g. if your parents complain that you did not like something at camp.
- We may need to share some information with our insurance company to make sure we have the right insurance cover.
- We may need to share information with others such as the Scout County or Headquarters if something goes wrong or to help with an inquiry. For example, if an Explorer was is injured on a Unit activity.
- We will only share your information with other people and organisations when we have a good reason. Exceptionaly, we may need to share it more widely than we would normally.

- We may use videos or images of you for the District website, social media and other promotional materials. This is to show prospective members what we do. We may use these photographs and videos after you have left us.
- We sometimes may use companies to handle your personal information such as On Line Scout Manager.

Your personal data that we collect will generally remain within Scouting and will be handled only by adults who have a real need to know the details. Again, if you have any concerns about any of the above, please contact your Leader.

The legal bit - our legal grounds for using your information

This part contains legal information about the legal grounds we rely on when handling your information as described above.

Legitimate interests

This means that we are using your information when this is necessary for our legitimate interests. We rely on this ground for a number of the ways, specifically in:

- Providing you with a Scouting programme.
- Looking after you and other Explorers.
- Telling people about Scouting and what we do e.g. we may use images of you in our materials, website or in our social media.
- Improving Scouting e.g. if we want to raise money for new equipment to make sure that we are providing you with a good Scouting experience.

Also, your personal information may be processed for the legitimate interests of other people such as investigating a complaint made by one of your fellow Explorer Scouts. If you object to us using your information where we are relying on our legitimate interests as explained above please speak your Leader.

Vital interests

In rare situations we may use your information to protect your vital interests or the vital interests of someone else (e.g. if you or they are seriously hurt).

Consent

We may ask for your consent to use your information e.g. taking photos. If we ask for your consent you can take it back at any time. Any use we have made of your information before you withdraw your consent will still remain valid.

There are some limited circumstances where your request to withdraw consent can't always be accepted. For example where we have to comply with Headquarters obligations to keep certain data.

Legal claims:
We are allowed to use your information in the case of any to legal claims – this would allow us to share details with our insurers and Headquarters.

We must also comply with additional conditions where we process **special categories of personal information**. These special categories include personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, and information about sex life or orientation. This information is kept securely and normally only available to your Explorer Scout Leader.

Sending information to other countries

We may have to send your information to countries without the same level of protection for personal information as there is in the UK e.g. a Scout event overseas. The European Commission has produced a list of countries which have good data protection regulations. Details can be found here.
If the country we are sending your information to is not on the list or, is not a country within the EEA (which means the European Union, Liechtenstein, Norway and Iceland) then, it might not have the same level of security for personal information as there is in the UK. In such cases we will provide you with details about the safeguards we will put in place in this situation.

Keeping your information

We will keep your information for as long as we need to provide a Scouting programme and look after you. We may keep some information after you have left the Unit, for example, so that we can find out what happened if you make a complaint.

In exceptional circumstances we may keep your information for a longer than usual, but we would only do so if we had good reasons and only if we are allowed to do so under data protection law.

We can keep your information for a long time or even indefinitely if we need it for archival records or statistical purposes. The table below shows for how long we keep different types of information.

Information type	Normal retention period
Accident and medical treatment records	Date of birth plus 25 years.
Complaints with Scouting	10 years and then reviewed.
Your progress record	5 Years.

What decisions can you make about your information?

Data protection legislation coming into force in May 2018 gives you rights about your information. Some of these are new whilst others build on your existing ones. Your rights are:

- you can ask for us to delete information we hold about you in certain circumstances e.g. where we no longer need it;
- if information is incorrect you can ask for a correction;
- you can ask what information we hold about you and be provided with a copy;
- you can ask us to send you certain types of information about you in a format that can be read by computer;
- our use of information about you may be restricted sometimes e.g. if you inform us the information is inaccurate we can only use it for limited purposes while we check its accuracy.

Further information and guidance

This notice explains how we look after your personal information. Please ask to speak to your Leader if you would like us to update your information or you would prefer that certain information remains confidential. If you consider that we have not acted properly when using your personal information you can contact the Information Commissioner's Office: ico.org.uk.

Date policy AGREED:
Next REVIEW date

5

Bishop's Stortford and District

Subject Access Request Process

For GSL's, Group Chairs, DESC, ESL's, DC and District Chair

Data protection law allows individual volunteers, parents and Explorer Scouts to have the right to see a copy of the information that local Scouting holds on them, subject to certain exemptions and limitations set out in the regulations. These rights are called a Subject Access Request (SAR). Data held by the National Headquarters is thier responsibility, not the District. A SAR entitles people to be:

- told if any personal data is being manged by the local Scouting;
- provided with a description of the personal data, why it is being processed, and to who else has it been given;
- provided with copy of the personal data; and
- told where the information came from (the source) if you know.

A SARs gives people the right to see only their own personal data not a right to see copies of documents that might contain their personal data. Sometimes the easiest way to provide the relevant information is to give copies of the original documents, but you are not obliged to do this. People are also are entitled to be:

- told why local Scouting processes their data;
- told about how long we intend to keep their data;
- told about rights regarding to erasing or amending their data;
- provided with a copy of the information with the data and given details of the source of the data (where this is available).
- told of the categories of the data you hold about them;
- told of any third parties who have, or will receive their data e.g. HQ, OSM;
- told if any data has been transferred overseas;
- told how to make a complaint to the Information Commissioner Office (ICO) should they be unhappy;

You must ensure that the person making the request is who they say they are and is legally entitled to make the request.

Before responding to a SAR from an Explorer Scout the District Commissioner and the Unit Leader must agree that they are mature enough to understand their rights. After discussion, if the DC and ESL feel the Explorer does understand their rights, Scouting can respond to them rather than the parent. What matters is the Explorer is able to understand what it means to make a SAR and how to understand the information they get as the consequences.

When considering borderline cases with Explorer, we must take into account:

- their level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any duty of confidence we may owe to them;
- if any court orders relating to parental access that may apply;
- any views of the Explorer on if their parents should see the information; and
- the consequences of allowing parents access to their information -particularly if there is a safeguarding allegation or ill treatment.

Bulk requests

In very rare circumstances, we may get lots or requests for a SAR at the same time – maybe if there has been an incident or data breach that gets media attaention. These are called “bulk requests”. Each SAR within a bulk request must be considered individually and responded to. We must note the following issues when dealing bulk requests:

- any SAR made as part of a bulk request has the same legal status as a SAR that is made individually;
- the request and purpose for which a SAR is made does not impact on its validity, we must respond to it;
- if the request is made by a third party on behalf of someone, we must be satisfied that the third party is authorised to make such a request;
- we must also satisfy ourselves as to the identity of the individual concerned; and
- we must respond to a request even if we hold no information about the individual.

Complaints to the ICO about how we handle a SAR take into account the volume of requests received by an organisation. The organisation’s size and resources are likely to be relevant factors.

The request

Remember, SAR’s do not have to be labelled as a “SAR request” do not even have to mention data protection e.g. an email that just says "Please send me copies of all emails you hold about me" is a valid subject access request. Leader must **always** immediately let the Group Scout Leader (Groups) or the DC (in the District) know when they receive such requests. **We has only one month to supply the requested data by law.** Once it is suspected as Subject Access Request may be being made, the process is that:

The Action
Receipt of a request The Leader informs the GSL/DC that they think a SAR has been requested.
Notify The GSL or DC must inform the Group/District Chair and respective Data Protection Lead who must know about the request.
Get some clarity The Group/District Data Protection lead contacts the subject to try and clarify what they require aiming to focus on the times and dates of requested search. If the relationship with the subject and the Group/District has broken down, this may be difficult. The attached template should be supplied to the subject to try and help.
Confirm what is needed The subject has confirmed what information they need. When the subject wants to withdraw consents on specific data sets then must be done by marking the records accordingly. Confirm what has been done with the requested. When the subject wants to delete any information this may be allowed subject to any exceptions which must be checked with HQ.
The Search If certain data information is required within 10 working days - A search must start immediately for all email data. This must be collated by the Group/District as an electronic format PLUS a Search all electronic files (PC’s and all devices) for data PLUS searches for paper data.

Final Preparation
The Group/District Data Protection Lead will redact and collate all the data to be handed to the data subject. **This must be completed within one month from the original request**. We must disclose all the subjects Personal Data within the scope of their request - there are only very limited exceptions. There is no exemption for embarrassing information e.g. negative comments made in emails from Leaders about the subject

Handover
The data will be handed to the Data Subject as agreed. Record what you do.

Please note
Some data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. Advice from HQ should always be sought.

Dealing with repeated or unreasonable requests

The law does not limit the number of SARs someone can make but it does give you some discretion when dealing with requests that are made at unreasonable intervals. We are not obliged to comply with an identical or similar request to one already dealt with unless a reasonable interval has elapsed between the first request and any new ones. The law gives us some help about unreasonable requests. It says we should consider the following.

- The type of data – this could include if it is particularly sensitive.
- The purposes of the processing – this could include whether the processing is likely to cause harm to the requester.
- How often the data is altered – if information is unlikely to have changed between requests, we may decide that you need not respond to the same request twice.

If there has been a previous request or requests, and the information has been added to or amended since then, when answering a SAR we are required to provide a full response to the request: not merely supply information that is new or has been amended since the last request.

Further information

The ICO produce a helpful code of practice on their website. If there is any doubt or concern about a request, legal advice must be sought from Headquarters.

Date AGREED:
Next REVIEW date

Bishop's Stortford and District

Subject Access Request Form

It would help us find your data you require if you would please complete this form. In the case of young people under 13 this must be a parent/career. Explorer Scouts can make this request provided that in the reasonable opinion of their Leader and District Commissioner, they have sufficient maturity to understand the request they are making. All subject access requests from Explorers will therefore be considered on a case by case basis.

Applicants full name:				
Subjects full name:				
Subjects full address:	Post code:			
Applicant Phone numbers:	Home:		Mobile:	
Subjects Date of birth:				

Your Data Search
It is important you give us a much information as you can about the data you want e.g. any specific dates, events or times for the search.
Your comments:

Please continue overleaf

Your comments continued:

Please email return this form to:

(INSERT THE CONTACT]

Subject Header: Subject Access Request:

Suggested email text:

Dear Mr and Mrs Smith,

Please find attached a Subject Access Request form and I am asking you to supply the information I am entitled to under the Data Protection Act 2018.

If you need any more information from me please let me know as soon as possible. I understand that the Group/Distroct will reply to this request within 30 calendar days from today.

Yours faithfully

[Your Name]

6

[insert name of Group]

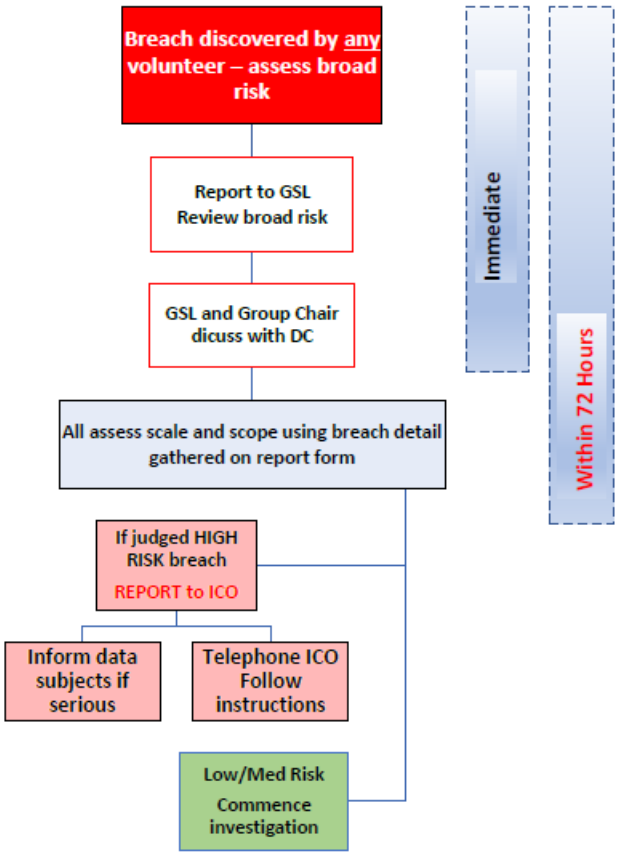
Note from Bishop's Stortford and District Scouting: a process like this is highly recommended in case of a data breach in your Group. The broad text is recommended and where there are [brackets] you need to insert your relevant Group information. If you have questions email the District Commissioner, Greg here.

Personal Data Breach Incident Procedures

For use by GSL and Group Chair

It is important that the Group Scout Leader and Group Chair read this procedure and be familiar with what to do if a data breach is reported to them. Under Data Protection Law, all organisations have a duty to report certain types of data breach quickly to the **Information Commissioner's Office** (ICO) and in some cases to the individuals affected.

Likely sequence of events



The Group must use appropriate technical and organisational measures to protect the personal data of members and volunteers including protection against *unauthorised or unlawful processing* and against *accidental loss*, *destruction* or *damage*.

For clarity the definitions are:

"*Damage*"	Where personal data has been altered, corrupted, or is no longer complete
"*Unauthorised Destruction*"	Where personal data no longer exists, or no longer exists in a form that is of any use to the Group.
"*Accidental loss*"	Where the data may still exist, but the Group has lost control or access to it, or no longer has it in its possession.
"*Unauthorised or unlawful processing*"	Includes disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the Law.

What breaches must the Group report to the ICO?

The Group needs to report a breach where it is likely to result in a *risk to the rights and freedoms of individuals*. If unaddressed, such breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This will be assessed on a case by case basis. An example would be if the Cub Leader lost a file with the leaders names, addresses and dates of birth. We would have to inform the ICO as this loss could leave individuals open to identity fraud. On the other hand, the loss or inappropriate alteration of a Leaders telephone numbers, for example, would not normally meet this threshold.

When would the Group have to notify individuals?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Group must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority. The GSL or Group Chairman, advised by the District will manage this process.

Informing the ICO

A notifiable breach **must** to be reported to the ICO within **72 hours** of the Group first becoming aware of it. The law recognises that it will often be impossible to investigate a breach fully within this time-period and allows organisations to provide information in phases. The law goes on to say that if the breach is sufficiently serious to warrant notification to the public, the Group must do so without undue delay. Where a notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay. Failing to notify a breach when required can result in a significant fine. The GSL/Group Chair will manage the communications and liaison with the ICO's office.

How will the Group inform the ICO?

The attached form is to be used (attached for Group Executive information only)

REMEMBER

The Information Commissioner's Office MUST be contacted within **72 Hours** of the first indication of a reportable breach.

When a Leader receives information about any breach, the [➔ *insert role (not name) of person responsible for the Group data Protection*]. **must be informed immediately- in this process every hour counts.**

Date AGREED:
Next REVIEW date

The [➔ *insert role (not name) of person responsible for the Group data Protection*] **will complete this form:** Provide as much information as possible and ensure that all mandatory (*) fields are completed – you can always go back to the ICO with information at a later stage.

1. ORGANISATION DETAILS:

***Our Group is:**	[➔Needs a contact address]
***Who is reporting breach to ICO:**	
***Your phone number and email:**	Phone: Email:
***Name of Group contact who should be the contact for the ICO:**	[➔ *insert role (not name) of person responsible for the Group data Protection*].
***Is the Group responsible for this breach:**	YES ☐ NO ☐ Don't Know ☐
***If NO which third party is responsible?**	Name and contact details:

1. DETAILS OF THE BREACH

(a) *Describe the nature of breach with as much detail as possible:

This breach is about:The categories of breach	✓
Unauthorised destruction	
Damage	
Accidental Loss	
Unauthorised or unlawful processing	

More details:

(b) *When did the incident happen:	

(c) *How did the incident happen:

(d) If there has been a delay in reporting to ICO why is this?

(e) *What measures did the Group have in place to prevent an incident of this nature occurring?

(e) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. PERSONAL DATA PLACED AT RISK

(a) *What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

	✓		✓	
Name		Date of Birth		**Other Please describe**
Address		NI Number		
Phone		Medical		
Email		Financial		

Other comments:

(b) *How many individuals are affected?	

(c)* Are the affected individuals aware that the incident has occurred?

Yes	
No	
Not sure	

(d) *What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the organisation about the incident?	
Yes	
No	
Not sure	

4. CONTAINMENT AND RECOVERY

(a) * Has the Group taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c)* What steps has the Group taken to prevent a recurrence of this incident?

5. TRAINING AND GUIDANCE

(a) Describe the training on Data Protection Act volunteer receive.

(b) Does the Group provide any detailed guidance to volunteers on the handling of personal data in relation to the incident being reported? If so, please provide any extracts relevant to this incident here.

6. PREVIOUS CONTACT WITH THE ICO

(a) Have the Group reported any previous incidents to the ICO in the last two years?	
Yes	
No	

If yes, provide brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. MISCELLANEOUS

(a) Has the Group notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Has the Group informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Has the Group informed any other regulatory bodies about this incident? If so, please provide details e.g. Charity Commissioners

(d) Has there been any media coverage of the incident? If so, provide details of this.

Form Completed by:	
Role:	
Date and Time of Completion	

Once completed, please telephone the ICO on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday) and send the completed form immediately to:

casework@ico.org.uk with '**DPA breach notification form'** in the subject field.

Next steps

When the ICO receive this form, they will contact us within seven calendar days to provide:

- a case reference number; and
- information about our next steps.

7

Revised 2nd May

Bishop's Stortford and District

Using Images of Young People Policy

Introduction.

This Policy provides information to parents and Explorer Scouts about how images of young people are normally used by Scouting. It also covers our approach to the use of cameras and filming equipment at events by parents and the media. The policy applies equally to Beaver Scouts, Cub Scouts and Scouts. It also takes account of data protection legislation and guidance from the Information Commissioners Office.

It also applies in addition to any other information we may provide about use of images, more general information about the use of young peoples' personal data and Privacy Notices.

Parents will be aware that from the age of 13 and upwards, the law recognises young people's own rights to have a say in how their personal information is used and this includes their images. For practical reasons, we apply this consent regulation when Scouts move to Explores but should any Scout aged 13 and over wish to assert their rights whist in the Troop, we will naturally support this.

General points.

As described in our Privacy Notices, we may take photographs or videos of young people at events to use on social media, on our website or other communications. We will rely on legitimate interests for this use. This helps us show prospective parents and members what we provide and to promote Scouting. We may seek specific consent from parents or older Scouts and Explorers before using a photograph or video recordings where we consider that the use is more privacy intrusive. We may continue to use these photographs and videos after your child has left us.

We hope that parents and Explorers will feel able to support us in using images to celebrate achievements and to promote Scouting.

Any parent or Explorer Scout who wish to limit the use of images should tell their Leader. We will respect such wishes wherever reasonably possible, and in accordance with this Policy.

Where we rely on consent, it will remain in place and be deemed valid until:

a. the young person leaves Scouting;

b. the young person reaches the age of 13 when additional pupil consent may be required; and

c. either the parent or young person withdraws consent at any time. Please be aware that it is only possible to remove online images and we cannot change printed materials once published.

Use of Images in Publications.

Unless the Explorer or their parent has requested otherwise, we will use images of young people to keep the Scouting community (parents, members, Leaders,) updated on our activities and for marketing and promotional purposes, including;

a) on internal displays (including clips of moving images) within our premises;
b) in communications within local Scouting including by email, intranet and by post; and
c) on our local Scout website and, where appropriate, via any social media channels e.g. Twitter, Instagram and Facebook. Such images would not normally be accompanied by the young person's full name without permission;

The source of these images will predominantly be our volunteers (all volunteers must use technology safely and responsibly in accordance with our Policy and Data Protection Policy).All images will be kept secure and safe.

Use of Images in the Media.
We occasionally supply images to the local media in certain situations e.g. Events, gaining awards. In the rare event that the media come to us and wish to take their own images, where practicably possible we will notify parents and Explorers in advance. We will make every reasonable effort to ensure that where permission has been refused for images, no such images will be provided for media purposes.

The media often ask for the names of the young people to go alongside the images, and these will be provided only where parents have been informed about the media's visit and either parent or Explorer has consented as appropriate. We would not normally use the full name, only the first name.

Security Images.
We take appropriate technical security measures to ensure images of young people held by us are kept securely and protected from loss or misuse. We will take reasonable steps to ensure that volunteers only have access to images of young people held by us where it is necessary for them to do so.

Use of Cameras and Filming Equipment (including mobile phones) by Parents.
Parents or close family members are welcome to take photographs of (and where appropriate, film) their own children taking part in our events, subject to the following guidelines, which we expect all parents to follow:

a) Parents are asked not to take photographs of other young people, except incidentally as part of a group shot, without the prior agreement of that child's parents or where appropriate the Explorer.

b) Parents are reminded that such images are for personal use only. Images which may expressly or not identify other pupils, should not be made accessible to others via the internet e.g. Facebook or published in any other way.

c) Parents may not film or take photographs in changing rooms, tents, nor in any other circumstances in which photography or filming may embarrass or upset young people.

d) We reserve the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from anyone who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

e) Leaders will question anyone they do not recognise who is using a camera or recording device at Scouting events.

Use of Cameras and Filming Equipment by Young People.
All young people are encouraged to look after each other and to report any concerns about the misuse of technology or any worrying issues to a Leader.

The use of cameras or filming equipment (including mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by young people in a manner that may offend or cause upset.

The misuse of images, cameras or filming equipment in a way that breaches this Policy, or the Association's Anti-Bullying Policy, Safeguarding Policy or procedures is always taken very seriously.

Further Advice
If you would like to contact us about any aspect of this Policy, please contact your Leader.

Bishop's Stortford and District

WHEN TO GAIN AD HOC CONSENT FOR IMAGES

Advice for Leaders

With changes to data protection legislation in May 2018, we no longer seek general consent for the use of young people's images (photographs or video recordings). We will instead, normally rely on regulations that give us what is termed *legitimate interest*. This is outlined clearly and transparently in our Privacy Notices and is also based on the reasonable expectations of parents about using images. It is important, when we use the grounds of legitimate interests to ensure we do so in accordance with our Privacy Notices and data protection policies and procedures. When using *legitimate interests* for taking images ask yourself the following questions:

a	**Are you taking this image for the Scouting?**	If not **STOP** – don't take it.
b	**Is the image particularly sensitive or private?**	**STOP** – is it <u>really</u> needed? If yes, you will need consent (see 7 below)
c	**Would parents reasonably expect you to be taking the image?**	Not sure? Read the Parent Privacy Notice. If still not sure don't take it.
d	**If challenged, are you happy to explain why you took it?**	No – then don't take it.
e	**Will the subject find its use intrusive?**	Not sure or yes? Either don't take it or seek consent.
f	**Will there be any impact or consequences for the subject?**	Discuss this with them and then ask for consent.
g	**Is the subject vulnerable in any way?**	If yes, discuss with safeguarding.

There are certain circumstances when specific consent **must** be obtained. In such cases, Explorer Scouts must provide consent - for all younger members, their parents provide consent.

Where consent is not required

You do not normally need to seek consent for a photograph like these:

(a) A group of Scouts, **without** names, published on a website or Group newsletter, which does not raise any of the factors in "borderline cases" (see below) which would make it more intrusive.

When used in on-line media where groups of Scouts are shown and names are included, the names should never be in the same order as the Scouts.

(b) Scouts on events or activities be used for **internal** display.

For example for the meetign place wall

(c) Photographs of the whole Section, to be given by parents.

(d) A group photograph of say 10 Beavers in the newspaper **without** full names.

Newspapers will always ask for names. You should only supply first name and surname initial. If full names are required and necessary we must always seek consent for the parent or student (over 13).

(e) Photo used only in a **Scouting newsletter** of a young person holding up, say a certificate or medal, even with a name.

Billy B 10th Blanktown gets chess award

Scouting should never publish images of young people in swim wear.

Where consent must be sought

You must seek consent for a photograph like these:

(a) Published in a newspaper alongside a member's name.

Ask
for Consent

We do not list the members names in the same order as the photo and normally only use first name and initial (unless consent given for full name)

(b) Published photo in e.g. newspaper alongside a Scouts town of residence or name.

Mat M living in from Bishops Stortford

Ask
for Consent

(c) In a Scout public publication or on a website with the members name.

Ask
for Consent

You should not normally use names on the website (unless a news story).

If used in social media with the **member's name**, e.g. on the Group Facebook page.

Ask *for Consent*

Any image linked to a name would need consent

(d) Used in a local advertising campaign with or without the member's name.

Ask *for Consent*

Any media where we use images of Scouts to promote or advertise Scouting.

(e) If you wish to publish a photo in **any media** where member are in revealing sports wear

NEVER publish images of young people that might compromise or embarrass them. Likewise too much skin on show, cleavage, micro skirts etc. are not accpetable.

Borderline cases for consent

There will always be borderline cases where it is not possible to be prescriptive and if in doubt ask first!

In every case, leaders should consider why the photograph or image is required and the impact on the individual. Decide whether consent is needed taking into account relevant factors, such as:

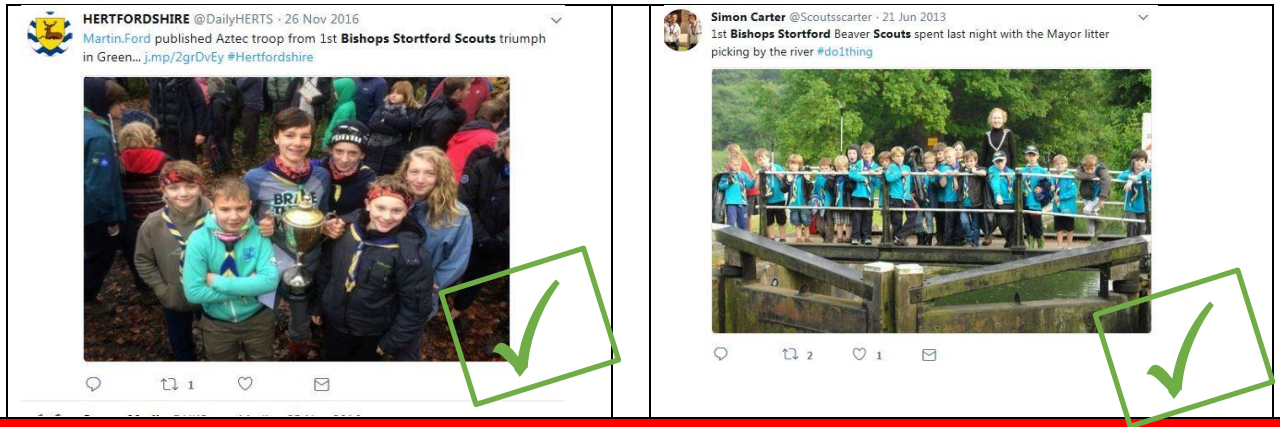
(a) **where the photograph is published** e.g. there is a difference between a photograph on the homepage of the Group website or appearing in a less prominent area of the website;

(b) the **age of the young person** - the younger the member, the greater the need for consent; and

(c) how the **young person is dressed** e.g. are they a revealing sportswear and prominently displayed in the photograph this suggests that consent should be sought.

These borderline cases include photographs used in **live social media.**

You <u>do not</u> need consent for images on social media such as these where no names are mentioned and it is a group



You <u>MUST</u> seek consent for these because they are close up face images or of one person and a name is mentioned in one post

In the above cases, immediate consent by way of a conversation (in person or by phone) recorded by an email afterwards should be sought. This can be from the Explorer or parent of younger members if present. If they are present you can use the **Ad Hoc Images Use form**.

If we know that photos will be taken for this purpose, advance planning may help. A quick email to all parents prior to the event saying that we <u>may</u> use e.g. twitter is being open and transparent. Leaders planning and running a camp or outing should seek permission to use images (subject to the policy) prior to the trip.

In summary if you are taking photos of young people ask yourself:

- Would a reasonable parent expect you to be taking this image as part of Scouting?
- Is the young person dressed appropriately and not in say, swim wear?

If you have **any doubt** or concerns, talk to [insert name of Group/District Data Protection contact].

Bishop's Stortford and District Explorer Scouts

Use of Your Image by the Scout District

This short form is used by Explorer Scouts when specific consent is needed for a particular image that is unusual e.g. full face phot for the newspaper

Dear Explorer,

You are at an age at which the law recognises that you have the maturity to provide your own consent to certain matters. We are entitled by regulations to use images taken of you and take decisions about how to use them, subject to any reasonable objections raised.

Occasionally, we need to seek specific consent from you before using certain personal data, photograph or video recording where we consider the use is more intrusive e.g. it may be **unusual** or **impactful** and has a **one-off** use. This form seeks your consent for such use, namely:

Your **image**:	[***insert purpose***]

Please indicate below if you are willing to consent for your image being used in this way. You may withdraw your consent at any time in the future, but please be aware that it is not possible to remove online images or change printed materials once published.

Yes, I agree to using my image in this way ☐

No, I do not agree to us my image in this way ☐

Name:	
Signature:	
Date of birth:	
Date:	

This completed form must be returned to [INSERT NAME]

Protecting your Privacy We will always take great care of your personal information. We use it as part of our operations and in accordance with current Data Protection legislation. For more information see our ***Privacy Notice for Explorer Scouts.***

[insert name of Group]

Use of Your Child's Image by the Scout Group

Dear Parent,

We are entitled by data protection regulations to use images taken of your child and take decisions about how to use them, subject to any reasonable objections raised.

Occasionally, we need to seek specific consent from you before using certain personal data, photograph or video recording where we consider the use is more intrusive e.g. it may be **unusual** or **impactful** and has a **one-off** use. This form seeks your consent for such use, namely:

Proposed use of **image**:	[***insert purpose***]

Please indicate below if you are willing to consent for your child's image being used in this way. You may withdraw your consent at any time in the future, but please be aware that it is not possible to remove online images or change printed materials once published.

Yes, I agree to using my image in this way ☐

No, I do not agree to us my image in this way ☐

Name of young person:	
Name:	
Signature:	
Date:	

This completed form must be returned to [INSERT NAME]

Protecting your Privacy We will always take great care of your personal information. We use it as part of our operations and in accordance with current Data Protection legislation. For more information see our ***Privacy Notice for Parents.***

8

Data and Privacy Protection text

1. **Joining Form in a Scout Group:** if you have one it is recommended that you add at the bottom no less than 9 point font:

Protecting your Privacy
We will always take great care of your personal information. We use it as part of our normal Scouting operations and in accordance with current Data Protection legislation.

By providing this information, you consent for us to use this data and to keep you and your child's information up to date. Where necessary, your data is made available the Group Trustees and other Leaders. We may need to share you and your child's details with the Scout District, County and National Headquarters.
Special category Personal Data
Where you have shared your financial details, your child's medical, special needs, racial, ethnic, religious or other beliefs information with us, it will only be shared with Leaders on a need to know basis.
For more information our ***Parents Privacy Notice*** can be made available to you.

2. **Joining Form in Explorer Scout Unit:** if you have one it is recommended that you add at the bottom no less than 9 point font:

Protecting your Privacy
We will always take great care of your personal information. We use it as part of our normal Scouting operations and in accordance with current Data Protection legislation.

By providing this information, you consent for us to use this data and to keep your information up to date. Where necessary, your data is made available the District Trustees and other Explorer Scout Leaders. We may need to share you and your details with the Scout County and National Headquarters.
Special category Personal Data
If you have shared with us your medical, special needs, racial, ethnic, sexual orientation, religious or other beliefs, information with us, it will only be shared with Leaders on a need to know basis.
For more information our ***Explorer Scout Privacy Notice*** which will be made available to you.

3. **Placing names on the waiting list** – in a confirmation email or form please add:

Protecting your Privacy
Thank you for registering your child to join our Scout Group. We will always take great care of your personal information and in accordance with current Data Protection legislation. We will use it to send you information about us and your details will be added to our records in order we can contact you about membership.
For more information our ***Parents Privacy Notice*** can be made available to you.