General Data Protection Regulations and IT Systems Acceptable Use Policies and Procedures

May 2019

Scouts

St Helens and District

Policy Contents

District Data Protection Policy

For St Helens and District Scouts

About this policy

N.B.: This Data Protection policy applies to all operations of St Helens and District Scout Council, including those at District Headquarters. It does not cover the operations of individual Groups, who should have their own policy.

The policy is designed to ensure that St Helens and District Scout Council complies with its obligations under the Data Protection Act 2018 and conforms to the following eight data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

N.B.: The District Data Protection Officer is the owner of this policy and responsible for regular revisions and updates as necessary.

This Data Privacy Notice/Policy describes the categories of personal data St Helens and District Scouts process and for what purposes. St Helens and District Scouts are committed to collecting and using such data fairly and in accordance with the requirements of the General Data Protection Regulations
(GDPR), the regulations set by the European Union, and Data Protection Act 2018 (DPA 2018), the UK law that encompasses the GDPR.

This Privacy Notice/Policy applies to members, parents/guardians of youth members, volunteers, employees, contractors, suppliers, supporters, donors and members of the public who will make contact with St Helens and District Scouts. St Helens and District Scouts are a registered charity with the Charity Commission for England & Wales; charity number 1053261.

The Data Controller for St Helens and District Scouts is the Executive Committee who are appointed at an Annual General Meeting and are Charity Trustees.

The Chair of the Charity Trustees is:

Mr. Frank Grayson
Email: frank.grayson@sthelensscouts.org.uk

The District Data Protection Officer (DPO) is:

Email:

The majority of the personal information we hold, is provided to us directly by you or by the parents or legal guardians of youth members verbally or in paper form, digital form, via our online membership system Compass or OSM. In the case of adult members and volunteers, data may also be provided by third parties, such as the Disclosure and Barring Service (DBS).

Where a member is under the age of 18, this information will only be obtained from a parent or guardian and cannot be provided by the young person.

We may collect the following personal information:

- Personal contact details such as name, title, address, telephone numbers and personal email address - so that we can contact you.
- Date of birth - so that we can ensure young people are allocated to the appropriate Section for their age and that adults are old enough to take on an appointment with Scouting.
- Gender – so that we can address individuals correctly and accommodate for any specific needs.
- Emergency contact information - so that we can contact someone in the event of an emergency.
- Government identification numbers e.g. national insurance, driving license, passport - to be able to process volunteer criminal record checks.
- Bank account details, payroll information and tax status information - so that we can pay any staff that might be employed by us and collect gift aid from HMRC where donations are made.
- training records - so that members can track their progression through the Scout programme or adult training scheme.
- Race or ethnic origin - so that we can make suitable arrangements based on members cultural needs.
- Health records - so that we can make suitable arrangements based on members medical needs.
- Criminal records checks - to ensure Scouting is a safe space for young people and adults.

We comply with our obligations under the GDPR and DPA 2018 by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.
In most cases the lawful basis for processing will be through the performance of a contract for personal data of our adult volunteers and legitimate interest for personal data of our youth members. Sensitive (special category) data for both adult volunteers and our youth members will mostly align to the lawful basis of legitimate activities of an association. Explicit consent is requested from parents/guardians to take photographs of our members. On occasion we may use legitimate interest to process photographs where it is not practical to gather and maintain consent such as large-scale events. On such occasions we will make it clear that this activity will take place and give individuals the opportunity to exercise their data subject rights.

We use personal data for the following purposes:

- to provide information about Scout meetings, activities, training courses and events to our members and other volunteers in St Helens and District Scouts
- to provide a voluntary service for the benefit of the public in a geographical area as specified in our constitution
- to administer membership records
- to fundraise and promote the interests of Scouting
- to manage our volunteers
- to maintain our own accounts and records (including the processing of gift aid applications)
- to inform you of news, events, activities and services being run or attended by St Helens and District Scouts
- to ensure and evidence your suitability if volunteering for a role in Scouting
- to contact your next of kin in the event of an emergency
- to ensure you have and maintain the correct qualifications and skills.

We use personal sensitive (special) data for the following purposes:

- for the protection of a person's health and safety whilst in the care of St Helens and District Scouts
- to respect a person's religious beliefs with regards to activities, food and holidays

for equal opportunity monitoring and reporting.

The retention policy and how we store each type of data can be found in the below tables:

The personal data we hold:

Data description	Personal data included	Stored using	Retention policy	Responsible officer
Information about our adult members	Contact information, appointments, training records, activity permits and awards. (Includes sensitive data, as defined)	For adult members - Compass Membership management system, provided by UK Scout Association	Retained whilst a current member. A subset of data is retained when a membership ceases in order to support the vetting policy should the person re-apply for membership	District Appointments Secretary / DPO / District Commissioner / District Training Manager
Information about Safeguarding incidents	Contact information and information regarding the nature of any allegation, the status and outcome of the investigation	Paper, Email and Electronic Files	Indefinitely	District Commissioner
Information about our event attendees	Name and address of group leader, name, DOB, special diet	Paper records and OSM	2 years from end of event. Aggregated summary statistics indefinitely.	Relevant ADC / Event Organiser
	Name and address of group leader, name, DOB, special diet and medical condition of each participant	Paper records and OSM	2 years from end of event. Aggregated summary statistics indefinitely.	Relevant ADC / Event Organiser

	Contact details, next of kin information, medical conditions and special diets. (Includes sensitive data, as defined)	Paper records and OSM	Destroyed after event, unless medical incident and then kept for 3 years.	Relevant ADC / Event Organiser
Information about general enquirers	Contact information and nature of enquiry, which may contain personal data	Email	Indefinitely	District Administrators / District Commissioner
Information about complainants	Contact information and nature of complaint, which may contain personal data	Email	Indefinitely	District Commissioner
Information about people registered to our mailing lists	Contact information	Email, Electronic Files and OSM	Indefinitely, unless the individual requests removal	District Commissioner / District Newsletter Editor

For completeness, we also hold the following information which is not categorised as Personal Data but has the following retention policies applied:

Data description	Retention policy	Responsible officer
Finance – purchase ledgers, record of payments made, invoices, bank paying in counterfoils, bank statements, remittance advices, correspondence regarding donations, bank reconciliation.	Indefinitely	District Treasurer
Finance – Receipt cash book and sales ledger	Indefinitely	District Treasurer
Finance - Fixed assets register	Indefinitely	District Treasurer
Finance - Deed of covenant/Gift aid declaration and legacies	Indefinitely	District Treasurer
Buildings – Deeds of title	Indefinitely	District Secretary
Buildings – Leases	Indefinitely	District Treasurer
Buildings – Documentation regarding plant and machinery	Indefinitely	District Secretary
Buildings – records of major refurbishments, warranties, planning consent, health & safety files.	Indefinitely	District Secretary
Trustee's minutes	Indefinitely	District Secretary
Annual accounts and annual reports	Indefinitely	District Secretary
Insurance policies	Indefinitely	District Secretary
Health and safety records	Indefinitely	District Commissioner

Our security policies

The following security policies will apply to the storing of personal data as outlined in this policy. These security policies are mandatory.

Overarching policies

Need to know – We only give people access to the data that they need to carry out their role. If people change roles, we review access accordingly.

Passwords – We use systems that force complex password complexity. Changed regularly or set once and keep until you think the password has been compromised.

Commercially available software – where possible we use third party software to store personal data (provided as software-as-a-service), where the software is regularly testing and patched for security vulnerabilities.

Transporting data – We only transport data using physical media if absolutely necessary and then using encrypted media only.

We keep people informed – we tell people why we are collecting their data and how we use it, at the point in time we collect it.

Physical storage

Limiting storage – We limit the amount of personal data we physical store to the absolute minimum. Only those with a need to know will have access to the data.

Locked – Physical documents with personal data will be store in a locked cabinet.

IT Acceptable use – Our IT Acceptable Use Policy outlines how we should use the charity's IT systems.

Boundary security – Our IT network shall have a boundary firewall which restricts inbound access to those ports and protocols specifically approved, which is maintained and supported.

IT Security patching – The latest available IT Security patches are installed regularly and automatically.

Virus – A virus scanning service is installed on all devices and regularly monitored.

File storage – documents containing personal data should only be stored using compass (adults) and OSM (children).

Encryption – All devices are disk encrypted.

Email

Acceptable use – Our IT Acceptable Use Policy outlines how we should use the charity's email system.

Restriction - Our volunteers should use a secure email system as their primary method for receiving, storing and sending of emails, and always when they are transmitting personal data.

Virus, Malware and Phishing protection – All emails will be scanned for virus, malware and phishing.

IT security - We rely upon the IT security provisions of Office 365 to provide an adequate level of security for our needs.

Volunteer equipment

Virus – A virus scanning service must be installed on all devices and regularly checked.

Removable storage – Removable devices that will contain personal data should be encrypted.

Third parties

Third party processing – Other than The Scout Association, we limit the use of third parties to process personal data collected by St Helens and District Scout Council and only do so where we have the express permission of the District Commissioner.

Third party compliance – We ensure third parties we contract with to store personal data comply with the principles of this policy, have an information security policy in place and ideally hold an information security standard (such as ISO 27001).

Limiting exports – When exporting data from third party systems (e.g. Compass, OSM), we only export the data we need for the purpose we need it for and destroy if immediately after it has been used for that purpose

Sharing your Data

Young people and other data subjects

We will normally only share personal information with adult volunteers holding an appointment in St Helens and District.

Adult volunteers

We will normally only share personal information with adult volunteers holding appropriate appointments within the line management structure of The Scout Association for St Helens and District Scouts as well as with The Scout Association Headquarters as data controllers in common.

All data subjects

We will however share your personal information with others outside of St Helens and District Scouts where we need meet a legal obligation. This may include The Scout Association and its insurance subsidiary (Unity Insurance Services), local authority services and law enforcement. We will only share your personal information to the extent needed for those purposes.

We will only share your data with third parties outside of the organisation where there is a legitimate reason to do so.

We will never sell your personal information to any third party.

Sometimes we may nominate a member for national awards, (such as Scouting awards or Duke of Edinburgh awards) such nominations would require us to provide contact details to that organisation.

Where personal data is shared with third parties, we will seek assurances that your personal data will be kept confidential and that the third party fully complies with the GDPR and DPA 2018.

Further Processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Your Rights

As a Data Subject, you have the right to object to how we process your personal information. You also have the right to access, correct, sometimes delete and restrict the personal information we use. In addition, you have a right to complain to us and to the Information Commissioner's Office (www.ico.org.uk).

Unless subject to an exemption under the GDPR and DPA 2018, you have the following rights with respect to your personal data:

- The right to be informed – you have a right to know how your data will be used by us.
- The right to access your personal data – you can ask us to share with you the data we have about you. This is a Data Subject Access Request.
- The right to rectification – this just means you can update your data if it's inaccurate or if something is missing. Adult members will be able to edit and update some information directly on The Scout Association's Compass membership system.
- The right to erasure – this means that you have the right to request that we delete any personal data we have about you. There are some exceptions, for example, some information will be held by The Scout Association for legal reasons.
- The right to restrict processing – if you think that we are not processing your data in line with this privacy notice then you have the right to restrict any further use of that data until the issue is resolved.
- The right to data portability – this means that if you ask us, we will have to share your data with you in a way that can be read digitally – such as a pdf. This makes it easier to share information with others.
- The right to object – you can object to the ways your data is being used.
- Rights in relation to automated decision making and profiling – this protects you in cases where decision are being made about you based entirely on automated processes rather than a human input, it's highly unlikely that this will be used by us.

Consent

Where we do not have a lawful basis to hold or process data, we will seek the express consent of individuals to hold data about them. This will be by specific and unambiguous statements that must be opted-into on any forms (electronic or otherwise) and systems. In some circumstances due to the organisation of the Scouts, we ask our members to ensure they have express consent for the data they are submitting to us.

In example for an event we are organising:

"I consent to my name, date of birth, and contact information to be used for the purposes of administering scouting activities in St Helens and District. We will not use this data for any other purpose than this event, except in aggregate to provide statistics for historical reference. We will delete this data one year after the event ends."

Data Subject Access Requests

Should a member of St Helens and District Scouts or a member of the public request a copy of any personal information which St Helens and District Scout Council holds, then the following process should be followed:

The individual should write to the District Commissioners Office outlining the personal data they are seeking to obtain who will refer to the Data Protection Officer.

The Data Protection Officer shall acknowledge the request by email.

The Data Protection Officer shall seek to verify the identity of the individual and that they are lawfully entitled to request a copy of the personal data. This may involve asking for information such as a membership number, date of birth, address, or documentary evidence.

The Data Protection Officer will collate the data requested, noting that we cannot provide data held by other organisations such as the Scout Association, County or Individual Groups. The data should be carefully analysed to ensure it does not refer to any other individuals, in which case it should be redacted.

Within 30 days of the receiving the request, the Data Protection Officer will provide the data to the individual. This will normally be by email.

For more information about our legal obligations, refer to the ICO website.

Right to erasure (Right to be forgotten)

Should a member of St Helens and District Scouts or a member of the public wish for their personal information to be erased, then the following process should be followed:

The individual should write to the District Commissioner outlining the personal data they are seeking to erase.

The District Commissioner shall consult the District Chair, District Secretary and DPO, to decide as to whether the request should be processed. Guidance from the ICO should be followed. Whilst St Helens and District Scouts will not seek to refuse the request unreasonably, it has a number of statutory obligations to comply with and uses personal data as part of its vetting and safeguarding procedures.

If it is deemed that the data shall be deleted, then the District Commissioner will confirm to the individual the timescales involved and instruct the necessary responsible officer to delete it.

Correcting inaccurate personal data

Should a member of St Helens and District Scouts or a member of the public believe that information that we hold about them is inaccurate, they should write to the District Commissioner outlining the inaccuracy. The District Commissioner will then seek to correct the data and confirm back to the individual.

Reporting a breach

A breach is defined as any event which “leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”. If a breach occurs, the District Commissioner should be immediately informed.

The District Commissioner (in consultation with the District Chair, District Secretary and DPO) will need to consider if the breach is likely to “result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage”. If it does, the ICO should be informed within 72 hours of the breach occurring.

If the breach results in a high risk to the rights of the individuals involved, they should also be informed directly

.

Data Privacy Management Procedure for St Helens and District Scouts

About this procedure

This procedure defines how St Helens and District Scout Council will manage personal data to assure appropriate data privacy in accordance with the UK Data Protection Act 2018. It should be read in conjunction with current information and guidance published by the UK Information Commissioner's Office (ICO – http://ico.org.uk/)

Note that once the UK leaves the European Union, additional requirements of the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) may continue to apply with respect to data processed relating to EU citizens, which may include members. As St Helens and District Scout Council does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the UK Data Protection Act 2018 will meet the requirements of the EU GDPR regulation. Should this position change this procedure will be reviewed.

The general requirements for data protection are defined in the District Data Protection Policy.

The general process for assuring data privacy is shown overleaf. This is supplemented by four additional procedures:

- Subject Data Access Request Procedure
- Subject Data Correction Request Procedure
- Subject Data Deletion Request Procedure
- Subject Data Breach Reporting Procedure

Step	Description
1. Identify Data	The Data Protection Officer is responsible for identifying all personal data, supported by the appropriate Responsible Officer (data owner) and other appropriate volunteers. For each set of personal data processed, the District data protection policy defines: • The data description • The personal data included • How and where data is stored • The data retention policy • The Responsible Officer (data owner) Where new data sets or changes to datasets (including data no longer held) are identified, the data protection policy should be updated to reflect the changes and steps 2 – 4 (and possibly step 6) repeated for the dataset
2. Identify and Document Requirements	For all personal data, the Data Protection Officer is responsible for identifying data protection and data privacy requirements supported by the appropriate Responsible Officer (data owner) and other appropriate volunteers or members of staff. These are generally based on the requirements derived from the UK Data Protection Act 2018. Where changes to personal datasets are identified (step 1 above) additional data protection/privacy requirements may be identified to comply with applicable jurisdictional requirements. Any additional such requirements should be documented.
3. Data Risk Assessment	The Data Protection Officer is responsible for ensuring that data privacy risks are identified, supported by the appropriate Responsible Officer (data owner) and other appropriate volunteers. Based upon the data identified in step 1 above and the requirements identified in step 2 above, data privacy risk assessments should be conducted to identify applicable processes and controls. St Helens and District Scout Council has determined that a general privacy impact assessment is required. This is documented in annex 1 below and general processes and controls have been considered to mitigate the risks identified in this generic privacy impact assessment. Such processes and controls have been developed in consideration of the general privacy impact assessment and implement established data protection / privacy good practices. It is not considered necessary to document detailed risk assessments where such good practices are followed. Specific risk assessments (in the form of data, system or platform specific privacy impact assessments) may be conducted and documented for specific data privacy requirements. See ICO guidance for examples of suitable data privacy impact assessments.

4. Establish Process and Controls	General data protection principles and controls are defined in the district data protection policy. General data privacy process and controls are defined in the following procedures: • Subject Data Access Request Procedure • Subject Data Correction Request Procedure • Subject Data Deletion Request Procedure • Subject Data Breach Reporting Procedure Where changes to personal datasets are identified (step 1 above), and/or where specific data privacy impact assessments are conducted the applicability of these general requirements, processes and controls should be reviewed to ensure that they are fully applicable. Where existing requirements, processes and controls are considered insufficient to assure data protection/privacy one of the following must occur: • Update processes and controls to include new requirements and mitigate risks • Implement specific (additional or alternative) processes and controls to meet specific requirements and mitigate specific risks
5. Manage / Process Data	Data processing will take place following defined processes and established practices and in accordance with the data protection measures defined in the district data protection policy. Any specific data privacy management actions will be conducted in accordance with the following procedures: • Subject Data Access Request Procedure • Subject Data Correction Request Procedure • Subject Data Deletion Request Procedure • Subject Data Breach Reporting Procedure In addition, the following rights must be respected: Right to Object Individuals should be informed of their right to object to data processing at the first point of communication i.e. the first email they receive, available on their first visit to a website etc. Individuals may object to: • Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). • Direct marketing (including profiling) • Processing for purposes of scientific/historical research and statistics. In these cases, processing must cease unless the scout district can demonstrate • Compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual (e.g. safeguarding of young people or compliance of other regulatory requirements) • the processing is for the establishment, exercise or defense of legal claims

	Objections to direct marketing must be acted upon immediately Right to Restrict Processing Process should be halted when a data subject as a legitimate right to block processing. During this 'block', data may be stored but not processed. Enough data should be retained to identify the block. This is applicable when: • An individual contests the accuracy of the personal data, processing should be restricted until we have verified the accuracy of the personal data. • An individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate • When processing is unlawful, and the individual opposes erasure and requests restriction instead. • If the district no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim. Right to Data Portability Data subjects may request a copy of their personal data portability when: They have provided to their personal data to the Scout District. The processing is based on the individual's consent (or for the performance of a contract); and when processing is carried out by automated means. Data should then be provided to the data subject (or transmitted to another data controller) in an open format e.g. .csv file, .txt file etc., without undue delay and within one month, unless the data is considered complex (see Annex 2).
6. Retain / Archive / Delete Data	Following the ending of active processing a decision will be made to either retain, archive or delete data as follows: • Retain data: For cases where data is no longer being actively updated, changed or added to, but which still needs to be referred to on a regular basis. Where this is the case, access controls and permissions should be updated to make data 'read only' where possible • Archive data: For cases where data is no longer being actively updated, changed or added to, and which does not need to be referred to on a regular basis (i.e. may be retained for statutory purposes, risk mitigation purposes etc.). Where this is the case, access controls and permissions should be updated to make data 'read only' where possible and the data should be moved to a suitable secure hard copy of electronic archive • Delete data: For cases where data no longer needs to be retained When considering the above it should recognised that data may progress through a natural life cycle (active processing ➔ retained ➔ archived ➔ deleted), possibly bypassing these steps. Data should not be retained beyond the retention period defined in the district data retention policy.

Annex 1 – General Data Privacy Impact Assessment

St Helens and District Scout Council has determined the need for a Data Privacy Impact Assessment (PIA). This is because the district:

- Collects new information about individuals, including data of a kind particularly likely to raise privacy concerns or expectations e.g. health records, criminal record checks or other information that people would consider to be private.
- Requires individuals to provide information about themselves
- May use information about individuals for a purpose it is not currently used for, or in a way it is not currently used
- Discloses information to third parties (legal and natural persons) who are part of the Scout Association or other statutory bodies, where there is a need to disclose such information to assure the safety or safeguarding of our members, staff or members of the public, or to manage complaints.
- May act against individuals based on personal data, which may have an impact in their employment or appointment status

St Helens and District Scout Council does NOT

- Collect information about or contact individuals in ways that they may find intrusive.
- Disclose any other personal information to organisations or people other than as described above.
- Use technology that might be perceived as being privacy intrusive e.g. the use of biometrics or facial recognition.
- Act against individuals in ways that can have a significant impact on them, other than as described above.

As a result of the above, the general data privacy risk assessment has been conducted:

Privacy Issue	Risks to Individuals	Compliance Risk	Associated organisational risk
Data inaccuracy	Right to be informed Right of access Right to rectification Right to object Right to data portability Right to erase Right to restrict processing	Inability to comply with applicable requirements of UK Data Protection Act 2018 (and EU GDPR) Inability to comply with Policy, Organisation and Rules of the Scout Association	Financial penalties Other enforcement actions Reputational risk
Data breach	Data confidentiality		
Data destruction	Right of access Right to object Right to data portability Right to erase		
Data retention and processing beyond defined period	Right to restrict processing		

In seeking to mitigate such risks, specific controls have been identified and documented in the district data protection policy.

Annex 2 – Complex Data Portability Requests

St Helens and District Scout Council considers the following data subject portability requests to be complex. Where this is the case, acknowledgment of the request should be provided to the data subject within 30 days of receiving the request and the data should be provided to the data subject (or an alternative data controller) as soon as possible, and always within 90 days of receiving the request.

- Any request involving multiple data stores from within the district (e.g. email accounts, OSM, Compass, files: [lists, folders, databases])
- Any request involving a district funded OSM subscription.
- Any request involving data held by district volunteers in personal (secure) storage locations

All other such requests are considered simple and the data should be made available or transferred within 30 days of receiving the request.

If in doubt, the Data Protection Officer, balancing the rights of the data subject and the ability of the district to transfer the data, will provide a definitive determination of whether a data transfer request is considered simple or complex.

Scouts
St Helens And District

GDPR
POLICY

Version:	2.0
Date created:	February 2020
Author:	C. Valentine-Burrows
Ratified by:	Executive Committee
Date ratified:	10th March 2020
Review date:	January 2021

Revision History:

Version	Date created	Date ratified	Author	Summary of changes
1.0	May 2019	June 2019	C. Valentine-Burrows	New Document
2.0	February 2020	March 2020	C. Valentine-Burrows	Amendment for the provision of the UK leaving the European Union