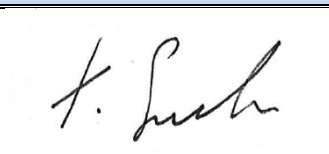
Data Protection Policy

Document Control

Date	Revision	Comments
1st October 2017	1	Initial issue
30th May 2018	2	V2
31th May 2018	3	V3

Produced By	Signed	Date
Tal Saunders		31st May 2018

Index

SECTION 1 - DATA PROTECTION POLICY STATEMENT

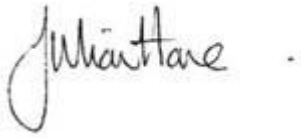
The amount of personal data about individuals which is held by people and companies has increased greatly in recent years. The European Union General Data Protection Regulations set out the rules for how personal data about living individuals should be held and used, particularly sensitive data such as racial or ethnic origin. The GDPR also gives individuals the right to find out what personal data is held about them either electronically or in a relevant filing system, and to see and correct personal data held. Or to have it removed or limited

All successful companies ensure that business risks are adequately controlled which includes risks resultant upon the mismanagement of data; we will ensure that we adequately comply with the principles set out in the General Data Protection Regulations

My responsibility is to ensure the effective implementation and maintenance of a robust Data Protection Policy.

This Policy will be reviewed regularly and updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations. Any revisions will be brought to the attention of all employees.

In case of any queries or questions in relation to this policy please contact Allium's Data Protection Officer; Mr Talek Saunders. Tel - 01872 276375
Email - DataProtection@allium.uk.net



Julian House
Director
Allium Environmental Limited **Date 31st May 2018**

SECTION 2 - INTRODUCTION

Allium Environmental Limited needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on our work. This personal data must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the General Data Protection Regulations

The following list of definitions of the technical terms we have used is intended to aid understanding of this policy.

Donor - The originating source of the data, for example, a client or contract frameworks

Data Controller – The entity who (either alone or with others) decides what personal data Allium will hold and how it will be held or used.

Data Processor – The entity that process the data on behalf of the Controller

General Data Protection Regulations – The EU regulations that provides a framework for responsible behaviour by those using personal data.

Data Protection Officer – The person(s) responsible for ensuring that it follows its data protection policy and complies with the General Data Protection Regulations

Data Subject – The individual whose personal data is being held or processed by Allium (for example: a client, an employee, a supporter).

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal data about her/him.

Notification – Notifying the Information Commissioner about the data processing activities of Allium, especially in the case of a breach where sensitive data may be compromised

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the General Data Protection Regulations

Processing – in relation to information or data, obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including

- Organisation, adaptation or alteration of the information or data;
- Retrieval, consultation or use of the information or data (which in relation to personal data, includes using the information contained in the data);
- Disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise available, or

- Alignment, combination, blocking, erasure or destruction of the information or data.

Personal Data – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Allium.

***Sensitive data* – means data about:**

- The racial or ethnic origin of an individual
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a Trade union
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.
- Any data that may put the identifiable person at risk of harm or malicious intent, or which may be used to discriminate.

SECTION 3 - DATA CONTROLLER

Allium Environmental Limited is a Data Controller under the GDPR, which means that it determines what purposes personal data held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

SECTION 4 - REGISTRATION

All personal information must be accurately summarised in our Data Protection register entry. A copy is held by us and is also published by the Information Commissioner's Office in Wilmslow on their website at www.ico.gov.uk. We must ensure that this register is kept up to date. To fulfil this requirement, all new and existing systems that contain information about individuals (both manual and computer systems) must be reported to Sarah House

SECTION 5 - DISCLOSURE

Allium may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware how and with whom their information will be shared. There are circumstances where the law requires Allium to disclose data (including sensitive data) without the data subject's consent.

Generally, information may be disclosed in the following circumstances:

- Where we are required to make disclosures by law (for example under anti-terrorism legislation) or in accordance with our legal duties (such as payroll information disclosed to HM Revenue and Customs), or under the direction of a Court Order.

- Protecting the vital interests of a data subject or someone else such as in a life or death situation.

- In connection with legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights.

- Where disclosures are allowed under the GDPR's exemptions, such as for the collection of taxes, the prevention or detection of crime, or the apprehension or prosecution of offenders.

A full list of circumstances where we may make disclosures can be found in Appendix 2 of the Staff Guide to Data Protection.

Disclosures may also take place to the individual to whom the information relates, or someone acting on their behalf such as a family member or legal representative, and our employees and those acting for us or on our behalf such as contractors and service providers, where such information is vital to their work.

Allium regards the lawful and correct treatment of personal data as very important to successful working, and to maintaining the confidence of those with whom we deal.

Allium intends to ensure that personal data is treated lawfully and correctly.

To this end, Allium will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulations

Specifically, the Principles require that:

1. Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met and only with the explicit consent of the subject.

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 purposes.

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

7. Appropriate technical and organisation 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.

Allium will, through appropriate management, strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information,

- Meet its legal obligations to specify the purposes for which information is used,

- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,

- Ensure the quality of information used,

- Ensure that the rights of people about whom information is held, can be fully exercised under the Regulation, These include:

    - The right of access to a copy of the information comprised in their personal data;
    - The right to object to processing
    - The right to prevent processing for direct marketing;
    - The right to object to decisions being taken by automated means;
    - The right to have inaccurate personal data rectified, blocked, erased or destroyed; and
    - The right to claim compensation for damages caused by a breach of the Regulation.

- Take appropriate technical and organisational security measures to safeguard personal data,

- Ensure that personal data is not transferred abroad without suitable safeguards,

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,

- Set out clear procedures for responding to requests for information,

- Contracts with service providers.

SECTION 6 - DATA COLLECTION

Informed consent, Informed consent is when:

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- And then gives their consent.

Allium will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. When collecting data, Allium will ensure that the Data Subject:

- Clearly understands why the information is needed

- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing

- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

- Has received sufficient information on why their data is needed and how it will be used.

SECTION 7 - DATA STORAGE

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers. Appropriate security measures will be taken to ensure that information and the equipment on which it is stored is protected from unauthorised access, accidental loss or damage.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately and securely.

It is Allium's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Keeping information secure means:-

- Effective password and User ID management
- Maintaining a system of regular back-ups and testing their effectiveness
- Using access controls such as restricted access on computer networks
- Maintaining up to date documentation of computer systems and programs, especially if any programs are written by us.
- Physical protection of equipment, to prevent theft or damage, in the office, in transit or at home.
- Protecting computers from viruses and other threats, by having up to date anti-virus software and internet firewalls.
- Secure transfer of confidential personal information by fax or email.
- Secure disposal of confidential and sensitive information.
- Procedures for prompt reporting of security incidents, or suspected breaches and dealing with them appropriately.
- Keeping an up to date and tested disaster recovery plan/business continuity plan.
- Ensuring the reliability of employees by carrying out appropriate checks during recruitment to determine their integrity and reliability, such as taking up references and verifying information provided on job applications.

SECTION 8 - DATA ACCESS AND ACCURACY

All Data Subjects have the right to access the information Allium holds about them. Allium will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Responsibilities

- Allium has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection,
- Everyone processing personal data understands that they are contractually responsible for following good data protection practice,
- Everyone processing personal data is appropriately trained to do so, at induction,
- Everyone processing personal data is appropriately supervised,
- Anybody wanting to make enquiries about handling personal data knows what to do,
- It deals promptly and courteously with any enquiries about handling personal data,
- It describes clearly how it handles personal data,
- It will regularly review and audit the ways it holds, manages and uses personal data
- It regularly assesses and evaluates its methods and performance in relation to handling personal data
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

APPENDIX 1

Staff Guide to Data Protection

1. Introduction

This guide is designed for all staff to assist them in ensuring personal information is well-managed and protected in compliance with the GDPR. It supports our Data Protection policy and staff training provision.

2. What does it apply to?

It applies to information relating to living, identifiable individuals. This can be automatically processed on computer or other mobile devices, as well as in structured manual records, such as paper files, closed circuit TV recordings, photographs, and audio recordings.

This personal information (known as personal data in the Regulation) is governed by the Regulation if an individual can be identified from it, or other information that is held, or is likely to be held by our organisation.

The Regulations does not apply to personal information relating to the deceased, companies or organisations, statistical, de-personalised or anonymised information.

3. Data Protection Principles

The General Data Protection Regulation consists of eight legally enforceable principles of good information handling practice and gives individuals legal rights, to safeguard their rights and freedoms.

These are, in summary; that personal information must be:-

- Processed fairly and lawfully and shall not be processed unless certain conditions are met
- Obtained for specified and lawful purposes and not further processed in a manner that is incompatible with that purpose
- Adequate, relevant and not excessive
- Accurate and where necessary kept up to date
- Kept for no longer than necessary, and not for an unspecified duration
- Processed in accordance with an individual's rights
- Kept secure, with adequate security precautions in place to prevent the loss, destruction or unauthorised disclosure of the information;
- Not transferred to countries outside the European Economic Area without adequate protection in place.

Processing means the organisation, alteration, retrieval, consultation or use of information, disclosure, dissemination, blocking, erasure or its destruction, in fact almost any action that you take when handling information.

Good Data Protection practice is all about effective information management and handling, from the time you decide to obtain it to its final destruction. By following our organisation's policies and procedures, respecting the rights of individuals, and ensuring their information is handled with care, the requirements of the Data Protection Act can be successfully met.

4. Ensuring Fairness and Acting Lawfully

Whenever you obtain personal information from individuals the Fair Processing Code should be followed, unless it is very obvious to them from the circumstances.

This means that you are open and transparent about what you intend to do with their information. They should be given some form of privacy policy or fair processing notice, either at that time or as soon as reasonably possible afterwards. You should ensure that they are not misled or deceived in any way. If you receive information about people from an external organisation or individual, consider whether they need to be informed about what you intend to do with it, unless this would be obvious to them or would involve disproportionate effort.

The notice or privacy policy should contain information about:-

- The identity of who they are giving their information to;
- What it may be used for – its intended purpose;
- Any other information that may assist in ensuring fairness to the individual, such as who it may be disclosed to, their rights and retention periods. They should also be given the opportunity to give their consent to any other secondary unrelated uses and direct marketing.

You do not have to provide a fair processing notice if the information is necessary:

- To record or disclose the information to comply with a legal obligation.
- For the prevention or detection of crime, or apprehension or prosecution of offenders.
- To carry out regulatory activities.
- Where information is made public by law.
- To protect the confidentiality of personal information for management forecasts/planning.
- As a record of the intentions of our organisation in relation to negotiations with the individual.
- If Legal professional privilege applies.
- For national security.

Acting lawfully means ensuring that whatever you do with personal information, you are not in contravention of other laws, such as Equality legislation, including any other criminal, civil, contract and common law. The General Data Protection Regulations states that you must satisfy specific conditions to process personal information, which means you have their consent, or other lawful justification. Extra care must be taken when using sensitive data. This is information relating to an individual's:

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.
- Any data that may put the identifiable person at risk of harm or malicious intent, or which may be used to discriminate.

A list of the conditions for processing are listed in Section 15, and must be adhered to. If you are unsure which condition applies, contact Tal Saunders.

A good example of common law is the common law duty of confidentiality – where someone has provided information to you in circumstances and on the understanding that it will not be disclosed further without their consent. If you disclose this information without consent or any other sound justification you would be processing their information unlawfully.

5. Managing Disclosures

The General Data Protection Regulation permits disclosures of personal information with consent and for other justifiable business and lawful reasons. A disclosure guide on circumstances when you can make disclosures is detailed within Section 16.

Care must be taken when disclosing personal information, whether it is verbally, by email, or letter to ensure it is disclosed on a need-to-know basis only. Security checks should take place to verify the identity of the person asking for it before information is released.

6. Information Sharing – *if organisation is involved in information sharing arrangements*

Individuals must be informed that their information is being shared routinely with other organisations unless there are justifications for not doing so for example if Allium Environmental Limited is under a legal obligation to share information, or for the prevention

or detection of crime or apprehension or prosecution of offenders, for example in relation to fraudulent activity.

There must be a legal basis for sharing information, a protocol or agreement in place that governs what information may be shared, and how it is shared, in accordance with the Data Protection principles.

7. Allium Environmental Limited Register Entry

We are required to register the use of the personal information that we hold with the Information Commissioner's Office. It ensures compliance with the second Principle where we are required to specify the purposes for which personal information is processed.

A COPY IS AVAILABLE TO THE PUBLIC ON THEIR WEBSITE AT WWW.ICO.GOV.UK

THE ACT REQUIRES THAT OUR REGISTER ENTRY IS ACCURATE AND KEPT UP TO DATE. FAILURE TO DO THIS IS AN OFFENCE. THE COMMISSIONER'S OFFICE MUST BE INFORMED WITHIN 28 DAYS OF OUR REGISTER ENTRY BECOMING INACCURATE. SARAH HOUSE IS RESPONSIBLE FOR MAINTAINING THE REGISTER ENTRY AND NOTIFYING THEM OF ANY CHANGES.

WE ARE REQUIRED TO PROVIDE A DESCRIPTION OF:-

- PURPOSE(S) FOR HOLDING PERSONAL INFORMATION
- TYPES OF PEOPLE ABOUT WHOM THE DATA IS HELD,
- TYPES OF PERSONAL INFORMATION HELD (SUCH AS FINANCIAL INFORMATION)
- RECIPIENTS – THOSE ORGANISATIONS OR INDIVIDUALS TO WHOM IT IS DISCLOSED,
- COUNTRIES TO WHOM IT IS TRANSFERRED OUTSIDE THE EUROPEAN ECONOMIC AREA OR WORLD- WIDE IF WE DISCLOSE TO A NUMBER OF COUNTRIES, FOR EXAMPLE BY PUBLISHING INFORMATION ON THE INTERNET.

TO HELP KEEP OUR REGISTER ENTRY UP TO DATE, YOU MUST NOTIFY TAL SAUNDERS OF:-

- ANY NEW COMPUTER AND MANUAL FILING SYSTEMS THAT YOU HAVE CREATED;
- SIGNIFICANT CHANGES TO EXISTING SYSTEMS (SUCH AS THE COLLECTION OF INFORMATION ABOUT A NEW CATEGORY OF PEOPLE)

- A CHANGE OF USE OR DISCLOSURE OF PERSONAL INFORMATION TO NEW **ORGANISATIONS OR MAKING** IT AVAILABLE ON THE INTERNET.

IT IS ESSENTIAL THAT WE ONLY CARRY OUT PROCESSING THAT IS DESCRIBED IN OUR REGISTER ENTRY.

8. Requests from people who want to see a copy of their own information

If you receive a formal request from someone who asks to see their information, pass it promptly to Tal Saunders. A formal request is normally in writing and refers to their right of access under the General Data Protection Regulation. They may also quote the Freedom of Information Act to you, as not everyone is aware which law it comes under.

It is important that you pass it the request on as quickly as possible as there is a strict time limit of 30 calendar days for Allium Environmental Limited to respond to a request.

Informal requests, or normal day to day business requests should be dealt with as usual, checking the requester's identity if you are in any doubt. For example, if a customer asks how much money they owe us, this information would be provided as part of a normal business request.

9. Other Rights

Notices

Individuals can also send us the following notices. If you receive one of these, pass it promptly to Tal Saunders who will deal with it.

- **Processing that may cause damage or distress -** An individual is entitled to serve a written "data subject notice" requiring us to cease or not to begin processing their personal information, where such processing is causing or is likely to cause unwarranted substantial damage or substantial distress to them or someone else.

- **Automated decision taking** - Individuals are entitled, by written notice, to require us to ensure that no decision that significantly affects them is carried out solely automatically, without involvement by people. Examples of automated decision-taking systems are computer systems that electronically evaluate matters relating to a person such as their performance at work, their creditworthiness, their reliability or their conduct.

- **The right to prevent processing for direct marketing purposes** - An individual is entitled to require us to cease or not to begin processing their personal information for the purposes of direct marketing. "Direct Marketing" is defined in the Regulation as meaning the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. It includes "host mailing" where advertising material is included in envelopes containing other correspondence for direct marketing purposes. Where direct marketing activities take place information that is sent by email, post, text message, unsolicited phone call or fax should only be done if the individual has consented

or been given the opportunity to opt out from being contacted for direct marketing purposes. The Privacy and Electronic Communication Regulations apply to direct marketing activities (even to businesses). Seek advice if you are involved in this activity and would like to know more about how these regulations affect your work.

Right to apply to a Court for rectification, blocking, erasure and destruction of personal information

Individuals have the right to apply to a Court for an order requiring us to rectify, block, erase or destroy information held about them that is inaccurate. This includes any opinions that are based on inaccurate information. The Court may also require us to notify third parties who may have been given the inaccurate information.

Seek Compensation

An individual who suffers damage or damage and distress as the result of contraventions of the General Data Protection Regulation is entitled to compensation through the Courts. Our organisation must be able to prove that we have taken such care as was reasonable in all the circumstances to comply with the Act's requirements.

Request an assessment by the Information Commissioner

An individual may ask the Information Commissioner to assess whether or not it is likely that any processing of personal information has been or is being carried out in compliance with the Data Protection Act.

10. Information Management

- Make sure that you only request or hold as much information as you need for the business purpose(s) that you need it. For example do not ask for an individual's date of birth, if "over 25" will suffice.

  However, be aware that the information should not be a bare minimum. Sometimes it is possible to be misleading by holding too little information. For example, the information that someone had a period of unemployment would be incomplete if the reason for the unemployment was that they were looking after a sick relation, and this was not recorded.
- Requesting information on the basis that it may be useful at some time in the future is not sufficient justification for holding information.
- Reasonable steps should be taken to ensure that changes in data or circumstances are recorded as soon as possible after an event and third parties should be notified promptly of any inaccuracies.
- Any opinions or remarks should be clearly marked, and always be of a professional nature.
- Where appropriate, record when personal information was last updated. The need to hold it should be reviewed on a regular basis, and a record of this should be made.

- For each system or collection of personal information set a review or destruction date. Review does not necessarily mean "delete" but there has to be a justification for records to be retained for a longer period. There are statutory requirements for certain information to be held for specified periods of time, for example financial records should be retained for 7 years. These requirements should be followed. A list of retention periods for information held is available within the Company's Combined Procedures Manual.
- Historical records, information held for research purposes or statistics can be held indefinitely provided the information is not processed to support measures or make decisions relating to particular individuals and it does not cause substantial damage or distress to them.
- If personal information is sent overseas (for example by email or published on the internet), an individual's consent should be obtained, or you should make sure you have another justification to do it. For example you can send information if it is to protect their vital interests, or if there are adequate protections in place in the country where the information is to be sent (such as a contract in place with the receiving organisation). For more information and advice on this, contact Sarah House.

11. Information Security

The General Data Protection Regulation requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of or damage to it.

It sets apart categories of information, known as sensitive data. Increased security measures must be taken to protect this information. Risk assessments should be carried out on all personal information, but in particular for sensitive data. You should identify possible security threats and vulnerabilities, the nature of harm or distress that may be caused to individuals if it fell into the wrong hands, was lost or damaged, what actions must be taken to protect it, what is technologically available to protect it and the cost involved.

Taking Personal information Out of the Office

Security measures must be in place when travelling and working out of the office. You should only take sensitive and confidential information home when necessary and use laptops and memory sticks that have encryption software on them.

In Transit

- Do not leave folders, paperwork or computer equipment on display in vehicles. Lock them out of sight in the boot of your vehicle.
- Take care when travelling in public places. Keep hold of computer equipment at all times. Disguise the fact that you are carrying a laptop if possible. Check behind you when leaving to make sure you have not left any paperwork or equipment behind.

Out of Office

- Lock personal information and computer equipment away when it is not in use.
- Ensure the computers you use are password-protected and have up-to-date anti-virus software, firewalls and network security in place. Wireless networks must be well-protected using lengthy passwords consisting of letters and numbers.
- Personal information and storage media should be securely destroyed when it is no longer needed. Cross-cut shredders should be used for paper.
- Personal information should only be accessed and used for Allium Environmental Limited business purposes, and not your own private use.
- Only use personal information that you are authorised to access and that is necessary for your work – do not discuss it in public places with colleagues or at home with family or friends – remember - "Walls have ears!"

Password Management

Passwords must not be shared and must be kept secure. They should be changed regularly, easy to remember but difficult to guess.

You should:-

- Avoid using two passwords and switching them. Use a different password every time.
- Try to use non-dictionary words - you can combine words or phrases (such as song titles), use numbers and other symbols.
- Change your password as soon as possible if you think someone knows your password.

Contingency and Disaster Recovery Planning

Allium Environmental Limited has a corporate disaster recovery plan for its computer systems and regular backups are taken and stored off-site. However if you use a laptop or computer that is not connected to the network and is stand alone, backups must be taken on a daily and weekly basis and a copy stored off-site, in case of fire or damage. Backups must be tested regularly to ensure they could be restored in the event of a disaster.

12. Service Providers and Organisations Who Process Personal information on our behalf

Allium Environmental Limited is legally responsible for the personal information that a service provider processes on our behalf.

For this reason there must be a written contract in place between us and a service provider that requires them to maintain the same levels of security that we do.

When selecting them, security guarantees must be requested that describe the security measures they will take, and controls that will be applied to protect Allium Environmental Limited personal information. It should include disclosures to third parties and what to do if a request is received from an individual who wants to see a copy of their information or to

exercise other rights under the General Data Protection Regulation or other legislation such as Freedom of Information law.

The contract should include the requirement for the service provider to act only in accordance with your instructions, and to allow you to inspect security arrangements, carry out audits and be given the right of access to premises and systems that process personal information. It should also specify what happens to the personal information when the contract ends or is terminated.

Section for Public authorities and business providing services on their behalf:-

13. Freedom of Information Act and Environmental Information Regulations

Anyone from anywhere can ask us for any information under this legislation. There are a number of exemptions where information may be withheld, including circumstances when the General Data Protection Regulations would apply. Requesters do not have to mention the Freedom of Information Act or Environmental Regulations when asking for information. There is a strict time limit of 20 working days for responses to requests.

If you receive a request for information from someone who wants to know about other people, for example how much specific staff earn, or details of complaints made to Allium Environmental Limited, it must be dealt with under the Freedom of Information Act. If it relates to any information held about the environment, it must be dealt with under the Environmental Information Regulations. In any event, pass the request promptly to Tal Saunders

Requests from people who want to see information that is held about themselves come under the General Data Protection Regulation and must be passed on to Tal Saunders.

Formal or informal requests – what's the difference?

Formal requests must be passed to Tal Saunders and they will respond to them in writing (or by email), within the requirements of the Freedom of Information Act or Environmental Regulations. They will confirm or deny that information is held and if no exemptions apply, will send the information to the requester within 20 working days.

You can generally identify formal requests as follows:-

- The request refers to the Freedom of Information Act or Environmental Information Regulations.
- The request is in writing (including emails) and formally requests information from you.
- You may be aware of reasons why the information should not be provided, for example, if release would breach one of the data protection principles, or the

information was given in confidence by someone outside Allium Environmental Limited.

- It is most likely that these reasons (and others) are covered by an exemption and may be withheld.

You can identify informal and normal business requests as follows:-

- The request was made verbally (although verbal requests are valid under the Environmental Information Regulations) and relates to information that you would routinely release such as who the contact is for Allium Environmental Limited.
- There is no duty of confidentiality owed to the people who the information relates to. The information was not provided in confidence.
- The information consists of publicly available information that is already in the public domain or common knowledge e.g. staff named on our website.

15. Lawful Conditions for Processing

The General Data Protection Regulation requires that you may **not** process personal data unless you can meet **at least one** of the conditions which are summarised below:-

Conditions for Processing Personal Data (Schedule 2 of the Data Protection Act)		
Individual has given their consent		
Processing is **necessary**: - • For the performance of a contract or for entering into a contract. • For the company to comply with any legal obligation. • To protect the vital interests of the individual (for example in matters of life and death) • For the administration of justice • For the exercise of any statutory functions carried out by the company required by or under law.		• For the exercise of any functions of the Crown, a Minister of the Crown or a government department. • For any other functions of a public nature exercised in the public interest • For the legitimate interests of the company or those of a third party to whom the data may be disclosed. This is information needed to carry out the work and business of the company provided it does not prejudice the rights and freedoms or legitimate interests of the individual. (For example if a person fails to pay money owed to the company, their name and address information may be disclosed to a debt recovery organisation).

If the information is sensitive data you must **also** meet at least one of the conditions in Schedule 3 below:-

Conditions for Processing Sensitive Personal Data (Schedule 3)	
Individual has given their **explicit** consent	▪ The information has been made public by the individual.
The processing is **necessary** :- ▪ For exercising or performing any right or obligation which is required by law in connection with employment. ▪ To protect the vital interests of the individual or another person – where the individual's consent cannot be obtained, given, or has been unreasonably withheld. ▪ For the legitimate activities of political, philosophical, religious or trade union not-for-profit organisations ▪ For the administration of justice ▪ In connection with legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights	▪ For the exercise of any statutory functions carried out by the company, required by or under law. ▪ For the exercise of any functions of the Crown, a Minister of the Crown or a government department. ▪ For medical purposes undertaken by a health professional or someone who owes a duty of confidentiality equivalent to that of a health professional. ▪ Racial or ethnic origin information that is only collected to monitor or review equality of opportunity or treatment, and with safeguards for the rights and freedoms of individuals

Sensitive data is:-

- the racial or ethnic origin of an individual,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

There are also certain circumstances where sensitive data may be processed without having to obtain explicit consent.

- **Equal opportunities and fair treatment** - For the identification or review of the existence or absence of equality of opportunity or treatment between persons with a view to enabling such equality to be promoted or maintained. This applies to information about an individual's religious or other similar beliefs, or their physical or mental health or condition. The processing of this information must not cause nor be likely to cause substantial damage or distress to the individual or any other person. If the information is to be used to support measures or decisions to be made about an individual, their explicit consent must be obtained.

- **Confidential counselling, advice, support or any other services -** Where processing is necessary in the substantial public interest, and it is carried out without the explicit consent of the individual.

- **Prevention or detection of crime** – must be in the substantial public interest, where seeking explicit consent of the individual would prejudice these purposes.
- **Discharge of any function designed to protect members of the public against dishonesty, malpractice or other seriously improper conduct**, **unfitness or incompetence** – must be in the substantial public interest.
- **Disclosure of information for journalistic, artistic or literary purposes,** with a view to publication can take place where our organisation believes that publication would be in the public interest.
- **Insurance or occupational pension schemes** where details of relatives of the insured person or member are required, (for example, health details of relatives used to calculate the life expectancy of the insured)
- **Political opinions by registered political parties**, provided such processing does not cause substantial damage or distress to any person.
- **Historical, statistical or research purposes,** for example, in the course of maintaining archives. The sensitive information must not be used to make a decision about an individual without their consent, nor cause them any substantial damage or distress.
- **Processing carried out by the Police** in the exercise of their common law powers

16. Disclosure Guide

If anyone requests information from you, ask yourself the following questions. Always make sure that you are satisfied that the requester is who they say they are. If in doubt, check it out - such as ask for evidence of identity.

Do you have the consent of the person to whom the information relates?

If they have consented, you can disclose (but it must be informed and freely given consent).

No consent? Have they been previously informed that you would make a disclosure (for example on a form collecting their information? If yes, you can disclose.

If you haven't informed them, would they legitimately expect you to disclose their information due to the circumstances?

Consider how the disclosure would affect them. If the information was provided in confidence, seek their consent first. Do not disclose if it would cause them or someone else harm or distress (unless you can satisfy any of the overriding justifications listed below in this document (for example the disclosure is required by law for child protection purposes).

Does the disclosure come under the Data Protection Act's Schedule 2 and 3 Conditions for processing, or other subordinate legislation? These permit "processing" of personal data (that includes disclosures) even if you do not have the individual's consent. For non-sensitive data, they are:

- For the performance of a contract, or with a view to entering into a contract with the individual,
- To protect the vital interests of the individual, for example to prevent serious harm to them or someone else, such as in a life and death situation.
- For the exercise of any functions of a public nature carried out in the public interest
- For the administration of justice
- For the exercise of any statutory functions carried out by an organisation, required by or under law.
- For the legitimate interests of Allium Environmental Limited or those of a third party to whom the personal data may be disclosed. This includes information needed to carry out the work and business of Allium Environmental Limited (and anyone else who you may disclose to externally). However, they must be legitimate interests (such as recovery of money that is owed to us), and the disclosure must not prejudice the rights and freedoms or legitimate interests of the individual whose information is to be disclosed.

For sensitive data:

- For exercising or performing any right or obligation which is required by law in connection with employment.
- To protect the vital interests of the individual or another person – where the individual's consent cannot be obtained, given, or has been unreasonably withheld.
- For the legitimate activities of political, philosophical, religious or trade union not-for-profit organisations
- For the administration of justice

- In connection with legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights.

- The information has been made public by the individual.
- For the exercise of any statutory functions, or disclosures required by or under law.

- For the exercise of any functions of the Crown, a Minister of the Crown or a government department.

- For medical purposes undertaken by a health professional or someone who owes a duty of confidentiality equivalent to that of a health professional.

- Racial or ethnic origin information that is only collected to monitor or review equality of opportunity or treatment, and with safeguards for the rights and freedoms of individuals

Other circumstances that are covered by subordinate legislation include:

- Equal Opportunities and fair treatment
- Confidential counselling, advice, support or any other services
- Prevention or detection of any unlawful act
- Discharge of any function designed to protect members of the public against dishonesty, malpractice or other seriously improper conduct etc
- For journalistic, artistic or literary purposes
- Insurance or occupational pension schemes
- Political opinions held by registered political parties
- Research purposes
- Processing carried out by Police Constables.

Is the requester acting on behalf of the individual?

Anyone can act on behalf of an individual, (such as their carer, guardian, friend, or solicitor) and receive information about them. If you are satisfied that they are genuinely acting on their behalf, in their interests, you may disclose. If not, ask for written confirmation with an indication that the individual has consented to the disclosure. Sometimes a requester may have legal authorisation if the individual is unable to give consent such as a Power of Attorney. Check that parents have parental responsibility before disclosing to them. Not all do, if there has been a break-up or divorce, and may not be entitled to receive information about a young person.

Are you disclosing information to someone providing a service or acting on behalf of our organisation?

You may disclose to them. Temporary staff, contractors and service providers need to have information or access to systems to carry out their work.

A written contractual arrangement should be in place that specifically includes Data Protection Act compliance, requirements to only act in accordance with your instructions, provide security guarantees, etc.

Is the information necessary for :

- **The prevention and detection of crime or**
- **Apprehension or prosecution of offenders**
- **Assessment or collection of any tax or duty or of anything similar to this?**

There must be a substantial risk rather than a mere chance that failure to disclose will noticeably damage these purposes. It is your responsibility to ensure you have reasonable grounds for believing this before releasing the information. There is no legal duty or requirement to disclose information for any of these purposes. Alternatively, you could ask them to obtain a court order which you are required by law to act upon.

Does a specific law require the information to be made available to the public, for example the Electoral Register? If yes, the information may be disclosed.

Are you required by law to disclose the information? (Under an Act, by any rule of law or by the order of a court?) For example, our organisation has a legal duty to disclose employee payroll information to HMRC under tax law.

It is your responsibility to make sure there is a sound justification for disclosing information. Do not disclose until you are satisfied that it is lawful to do so.

If someone requests information from you, ask them to give you the specific statutory requirement to disclose, in writing, on their headed paper - including the Act under which they are requesting it. Seek advice if in any doubt. If a court order is presented to you, check what is being requested and only supply that which is written on the order.

Is the information needed in connection with legal proceedings?
Information may be disclosed, where it is **necessary**:

- for the purpose of, or in connection with any legal proceedings (including future prospective legal proceedings)
- for the purpose of obtaining legal advice
- for the purposes of establishing, exercising or defending legal rights.

  Disclosures must be "necessary" for the requested purpose. You are not obliged to make a disclosure and Schedules 2 and 3 of the Data Protection Act must still be complied with. It is your choice. You could ask the requester to seek a court order if you do not wish to disclose.

Is disclosure necessary to safeguard national security?

A certificate of exemption, signed by a Minister of the Crown is conclusive evidence of the requirements for this exemption having been met. It may identify the personal data requested in general terms and may have effect at the time or in the future. As always when making a disclosure you should make a record of what information was disclosed, who they were made to, when, and for what reason.

Is the information required for research, statistical or historical purposes?

Information obtained may be disclosed for these purposes if :-

- The information is processed (such as disclosed) exclusively for these purposes,
- The information is not processed to support measures or make decisions relating to particular individuals and
- It does not cause substantial damage or distress to them.

You should comply with the rest of the Data Protection Act, such as provide information to individuals whose personal information has been obtained for the above purposes, as to why the information is being collected, and the purposes for which it will be used. Information held for these purposes may be held indefinitely; you can use it for these purposes even if they are incompatible with its original purpose and the subject access right does not apply as long as results of research or statistics do not identify the individual.