E-ACT

DATA PROTECTION POLICY

This policy regulates the way in which E-ACT obtains, uses, holds, transfers and otherwise processes personal data about individuals and ensures all of its employees know the rules for protecting personal data. Further, it describes individuals' rights in relation to their personal data processed by E-ACT. For the avoidance of doubt, references to E-ACT shall be references to E-ACT, the E-ACT Free Schools Trust and all E-ACT Academies (including those in partnership within E-ACT, including free schools, specialist schools and feeder primary schools).

E-ACT abides by UK data protection laws, including the Data Protection Act 1998 ("the DPA"), in its handling of personal information. We aim to ensure our employees are acting in accordance with these laws and the relevant regulatory guidance and best practice. Those requirements, together with this policy, ensure that all employees of E-ACT fully understand E-ACT's obligations to comply with the DPA and other privacy laws and regulations of the UK.

Where E-ACT controls other entities (whether by virtue of contract, partnership, ownership of shares or otherwise), those other entities will be required to abide by the principles set forth in this policy.

What is Personal Data?

Personal Data is any information (for example, a person's name) or combination of information about a living person, which allows that living person to be identified from that information (for example a first name and an address).

Examples of Personal Data which may be used by E-ACT in its day to day business include names, addresses (e-mail and postal addresses), telephone numbers and other contact details, CVs, , photos and images, performance reviews, payroll and salary information. The definition also includes opinions, appraisals or intent regarding individuals (eg. employees, job applicants, students, parents, personal contacts at suppliers and individual members of the public).

The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in e-mails, on IT systems, as part of a database or in a word processed document) or on paper records (for example, in paper files or filing cabinets).

What activities are regulated by this policy?

E-ACT processes Personal Data on its employees, pupils, students, parents, carers, agents, the employees of its suppliers and any other individuals, including job applicants and former employees, for a multitude of purposes, including:

- Recruitment
- Employee performance management and professional development
- Payroll, fund management and accounting
- Business and market development
- Building and managing external relationships
- Research and development
- Planning and delivering of education and training (including, for example, pupil/student progression rates)
- Staff and student support and facilities management
- Knowledge management
- Research
- Sponsorship funding
- Other purposes required by law or regulation.

Other purposes for which E-ACT may process your personal information are set out in the public notification of E-ACT on the Register of Data Controllers which can be found on the website of the Information Commissioner's Office, at www.ico.gov.uk.

When we collect, store, use or erase Personal Data for any of these purposes, this is called **processing**. If you read, amend, copy, print, delete or send Personal Data to another entity (whether within your local academy or free school, within E-ACT as a whole or where that entity is not within E-ACT) this is a type of "processing" and is subject to the guidelines set out in this policy.

Why should I worry about complying with this policy?

Data protection laws are enforced in the UK by the Information Commissioner's Office ("the ICO"). The ICO can investigate complaints, audit E-ACT's processing of Personal Data and can take action against E-ACT (and you personally in some cases) for breach of the DPA and other relevant privacy laws. Such action may include making E-ACT pay a fine and/or stopping the use by E-ACT of the unlawfully processed Personal Data, which may prevent E-ACT carrying on its education activities. Entities which are found to be in breach of the DPA and other privacy laws also often receive negative publicity for the breaches which affects the reputation of E-ACT as a whole.

Each E-ACT staff member or Third Party is required to read and comply at all times with this E-ACT Data Protection Policy ("the Policy"). In this Policy a "Third Party" is anyone who is not an employee of E-ACT, for example agents, external organisations, consultants, contractors, and service providers.

What does "fair and lawful use of Personal Data" mean?

One of the main data protection obligations requires E-ACT (and its employees) to process Personal Data fairly and lawfully. In practice, this means that E-ACT (and each

employee) must comply with **at least one** of the following conditions when processing Personal Data:

- The individual to whom the Personal Data relates has consented to the processing;
- The processing is necessary for the performance of a contract between E-ACT and the individual;
- The processing is necessary to comply with a legal obligation placed on E-ACT;
- The processing is necessary to protect a vital interest of the individual; or
- The processing is necessary in order to pursue the legitimate interests of E-ACT and is not unfair to the individual or otherwise disproportionate to the benefits gained from the processing.

Reliance on this last condition in "the legitimate interest of the business", must be discussed with your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department], as there are various lawful reasons for processing. Consent for use is limited to the tasks set out in the consent provided to the individual.

If in any doubt about the fair or lawful use of Personal Data, you should contact your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department].

If you want to make a new use of any details held by E-ACT, you must not do so unless that new use satisfies one of the lawful reasons for processing and it is described in the relevant privacy notice provided to an individual (see below). For example if someone provides their details as a parent / carer for student support purposes, you may not be able to start sending them marketing e-mails unless that is covered in an appropriate notice and consent from that individual.

What is a Privacy Notice?

For data processing to be considered "fair", when an individual gives E-ACT any Personal Data about him or herself, E-ACT must make sure the individual knows who E-ACT is and what E-ACT intends to do with the Personal Data provided to it.

You should give individuals appropriate privacy notices when collecting their Personal Data. This means that E-ACT has to inform individuals about the processing of their Personal Data at (or before) the time the data is collected. You should therefore check whether there is an applicable notice, which covers the processing you, intend to carry out for E-ACT. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

Privacy notices must, by law, include information about which data is being collected, who holds the Personal Data, who is the Data Controller, what is the purpose of processing the data, and information on any disclosure to third parties.

If you have any questions about privacy notices, or wish to undertake a new project, which involves a change in the way individuals' Personal Data, is processed by E-ACT, please contact your local Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department].

Even with consent, or if one of the other lawful reasons for processing applies, E-ACT cannot make any use it wants of Personal Data. All the other rules explained in this Policy still have to be complied with. For example, E-ACT still has to satisfy the other requirements described below such as making sure the information collected is not excessive. Simply because a person has consented to giving you their information does not override the other requirements of this Policy, or the laws applicable to E-ACT. Similarly Personal Data must not be used in a way which would infringe another law. For example for bribery, or racial, age, sexual, or disability discriminatory purposes.

Where collecting personal data about an individual indirectly (eg from a published source), E-ACT must still inform the individual that it holds the data and the purposes for which that data will be used.

What is Sensitive Personal Data and what conditions need to be met when processing it?

Sensitive Personal Data is personal data about a person's race or ethnicity, their health (eg SEN data, child protection plans), their sex life, their religious beliefs, their political views or trade union membership, their physical or mental health or condition, their commission (or alleged) commission of any offence and any proceedings against them in this respect.

Sensitive Personal Data on staff or students should not be collected or otherwise processed unless essential to do so. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept more securely. Additional restrictions are placed on top of the lawful reasons for processing mentioned above. For example, consent of the individual has to be **explicit** (implied consent is not sufficient), and obtained prior to processing any Sensitive Personal Data.

E-ACT does not generally seek to obtain Sensitive Personal Data unless:

(i) The individual concerned agrees in writing that E-ACT may do so, on the basis of a full understanding of why E-ACT is collecting the data;

(ii) E-ACT needs to do so to meet its obligations or exercise its rights under employment law; or

(iii) In exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned.

Employees should note that the "legitimate interest" criteria described above is not valid when processing Sensitive Personal Data. Sensitive Personal Data should not be collected for any new purposes without the involvement of and approval from your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department].

Obligations on processing relevant data and keeping it accurate?

The Personal Data (including any Sensitive Personal Data) you collect should be appropriate to, and sufficient for, the relevant purpose(s) you are collecting it for, but not excessive for that purpose(s). Only process the data, which is necessary for the task; minimise your use of Personal Data rather than maximising it. **Do not collect and process more Personal Data than you really need.** In the end, it simply adds to E-ACT's compliance burden. For example, if you will never telephone someone at home, you do not need their home telephone number.

In addition, you must take care to record and input Personal Data accurately. This is important. There can be serious problems if Personal Data is incorrect. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. If not there may be serious problems. For example, a renewal or termination notice for a contract may be sent to the wrong address and may not be valid.

Data retention: How long should I keep Personal Data?

E-ACT cannot keep or retain Personal Data forever. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). Other records must only be kept while in current use and for a reasonable period afterwards.

As a general rule, when Personal Data is no longer needed by E-ACT for the purposes for which it was collected, this Personal Data should be securely destroyed (eg shredded) as soon as practicable. Any proposed destruction of data must be discussed with your line manager or your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] prior to any decision being made.

What are the Individuals' rights?

Individuals have certain rights in relation to their Personal Data:

- The right to access Personal Data held about themselves;
- The right to prevent processing of Personal Data for direct marketing purposes;

- The right to have Personal Data corrected;
- The right to compensation for any damage/distress suffered; and
- The right to be informed of automated decision making about them.

Should you receive a request from an individual to correct their details, to withdraw their consent to use their Personal Data or for E-ACT to stop certain uses of their Personal Data, you must inform your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] promptly and follow their instructions.

Individuals are allowed to withdraw their consent to E-ACT's use of their Personal Data at any time. If an individual contacts you to withdraw consent, inform your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] promptly and stop using / processing that Personal Data in a way that is inconsistent with the withdrawal of that consent until you have received guidance from your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] as to the necessary steps to be taken.

If you receive a request to stop sending direct marketing materials, you should cease sending further direct marketing communications to that individual pending guidance from your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] as to next steps. Such next steps will clearly depend on the particular context but in the scenario given above this may include adding that persons' name to a marketing suppression list rather than simply deleting their details entirely from the relevant database.

Requests received for access to Personal Data

Individuals can also ask for copies of the Personal Data E-ACT holds about them and other details about how E-ACT uses their Personal Data.

On receipt of a written request from an individual for access to his/her Personal Data, E-ACT will:

(i) Inform that individual whether E-ACT holds Personal Data about him or her;

(ii) Describe the data it holds, the reason for holding the data and the categories of persons to whom it may disclose the data; and

(iii) Provide the individual with copies of the personal data held about him or her, together with an indication of the source(s) of the data.

If you receive such an access request, there are special legal rules which must be followed as part of this process. Therefore, please pass the request on to your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently

head of Legal department] immediately and follow their instructions. You must not deal with such requests yourself.

If you receive a written request for other information about E-ACT, it may be a valid request for information under the Freedom of information Act 2000 or the Environmental Information Regulations 2004. In each case E-ACT is under a strict obligation to respond within a specific statutory deadline. Please pass any written requests for information (which do not amount to subject access requests, as set out above) to your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] immediately and follow their instructions.

What kind of security measures might be appropriate?

E-ACT must keep all Personal Data (including Sensitive Personal Data) secure. This means that the Personal Data must be protected against being accessed by other companies or individuals (for example, via hacking), from being corrupted or being lost or stolen. The Personal Data must also be protected so the wrong people cannot read or use the details. This applies to details in IT systems, e-mails and attachments and paper files. This is why, for example, you have a password and controlled access rights to IT systems. You must comply with E-ACT's security procedures (including the ICT Information Services Policy and ICT Acceptable Use Policy) whenever you handle Personal Data. E-ACT relies on you to keep data secure and for data security. Otherwise, there can be serious problems; for example, pupil/student SEN data could be leaked causing significant damage and distress.

If you work away from E-ACT's premises, you must comply with any additional procedures and guidelines issued by E-ACT for home working and/or offsite working. You must read these procedures and guidelines before processing any Personal Data away from E-ACT premises.

Extra care is needed to secure Sensitive Personal Data because more damage is likely if it is lost. For example, if details of an individual student's medical conditions got into the wrong hands it would be very distressing for that student. Be especially careful if you want to send Sensitive Personal Data to another person - including where by fax or e-mail - that it is sufficiently secure and can only be received and accessed by the intended recipient. **Do not load Sensitive Personal Data onto unencrypted storage devices such as memory sticks, flash drives or CDs**. Please read E-ACT security procedures (including the ICT Acceptable Use Policy) for more information.

E-ACT also recognises that adequate security is important where it arranges for outside service providers to process Personal Data on its behalf. Where such arrangements are established by E-ACT, service providers must be bound by written contracts to protect the Personal Data provided to them. See the section "Can I disclose Personal Data to Third Parties?" below for more information.

What should I do if I lose Personal Data or I think there is a data security breach?

There are potentially significant repercussions for E-ACT and the individuals affected arising from a security breach. Where a security breach arises you must:

- **Immediately** report the details to your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] providing them with as much information as you have available;
- Follow their guidance on dealing with the security breach and keep them up to date with any further information about it that you become aware of;
- Not approach any individual data subjects, customers, regulators or make any public announcements about the security breach incident without the prior agreement of E-ACT Central compliance officer [Currently head of Legal department].

Can I disclose Personal Data to Third Parties?

A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. **You must not disclose Personal Data to a Third Party outside E-ACT** unless that disclosure constitutes a lawful reason for processing and satisfies the information notice requirements as explained above. Your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] will be happy to discuss this with you.

There are some exceptions to deal with disclosures such as those requested lawfully by police where the information is necessary to prevent or detect a crime. If you receive a request for information about an individual from the government, police or other similar bodies or from journalists or other investigators you should pass that request immediately to your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] to be dealt with. The application of the relevant exceptions needs careful consideration. The burden is on E-ACT to determine whether these apply. Disclosure (however well meaning and however seemingly authoritative the requestor) without checking risks placing E-ACT in breach of several obligations under data protection legislation.

Access to Personal Data must be restricted to those employees of E-ACT and Third Parties who need to access it in order to perform their role. You must only process Personal Data where and to the extent you need to see and process it to carry out your job / role properly.

Can I send or transfer Personal Data overseas?

The DPA contains special rules on whether Personal Data collected in the UK can be transferred to another country. Within the UK, there are restrictions on the transfer of

Personal Data outside of the European Economic Area (such a transfer can happen, for example, where Personal Data is e-mailed outside the EEA). This is to make sure the Personal Data remains safe and the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

The fact that there will be transfers of Personal Data to other countries, especially to outside the EEA, should be clearly set out in the privacy notices described in the fair use section of this Policy above so that it is expected by the affected individuals.

Please note that any use of cloud computing technologies is likely to involve overseas transfers of personal data. For more information on cloud computing and overseas transfers please contact your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department].

What about the use of Personal Data for marketing purposes?

As with other types of processing, the use of Personal Data for marketing purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent. You therefore should not use Personal Data to contact individuals for marketing purposes (including sole traders and individual members of business partnerships) by e-mail, text or similar unless the individual has consented to marketing use. Individuals have a right to decline postal marketing. Where marketing is to be by e-mail, text or similar, the consent must clearly cover marketing by e-mail, text or similar. Special rules apply to how consent is obtained (for example, whether individuals can "opt out" of or "opt in" to receiving marketing) depending on the type of marketing contemplated and the means of communication with the individual.

It is advisable to check the scope of any marketing consent you are relying upon, particularly if you are sending information relating to Third Parties or contemplating sharing the Personal Data with a Third Party to allow them to do so. Please also see the sections on Data Disclosure and Exports of Data in that event. If you are obtaining Personal Data from a Third Party for marketing use, then you should check that the consents they have obtained permit the intended processing by E-ACT.

You must comply with any request by an individual not to receive direct marketing (where it is addressed to them) or their choice not to receive marketing by a particular method (for example, post, fax, telephone, e-mail or text messaging).

You must liaise with your Academy data protection officer [Paul Boobyer] or E-ACT Central compliance officer [Currently head of Legal department] about any marketing plans and follow their instructions.