DATA PROTECTION POLICY

EPT Document Control

This policy applies to all Education Partnership Trust Schools.

Date of last review	September 2018
Date of next review	September 2020
Policy status	Statutory
Owner	Governing Body/ Board of Directors
Lead Contact	Helen Rawnsley

Employers must:

- meet the legal requirements of the Data Protection Act 1998 and comply with the eight data protection principles.
- have procedures in place and operating to ensure appropriate use, disclosure and protection of personal data, including sensitive data relating to members of staff
- have procedures in place and operating in respect of pupil records.
- ensure that staff are aware of their rights under the Act.
- ensure that staff are aware of their responsibilities in relation to personal data of staff and pupils
- have procedures in place to respond to requests for access to personal data.
- have systems in place to rectify or erase inaccurate data.

Employees' Duties

Employees must:

- follow the procedures put in place against unauthorised access to, or use, loss or destruction of personal data
- use the designated procedures to make requests about personal data and access to their data
- respect the confidentiality of information provided by or on behalf of job applicants when involved in recruitment procedures
- inform the employer of any changes to their personal data which the employer would not otherwise be aware of.

In Practice
Overview

The Data Protection Act 1998 came into force on 1 March 2000. It replaces the previous Act of 1984 and was drawn up to comply with the EC Data Protection Directive, which was adopted in 1995.

Personal data is information about living individuals that enables them to be identified. The processing of personal data and the right of individuals to access it are protected by the Data Protection Act 1998. Anyone who processes personal data, whether held on a computer or in paper files, must comply. Potentially, all data held about staff or pupils can be inspected and must be processed fairly.

Freedom of Information Act

The Freedom of Information Act 2000 came into force on 1 January 2005. The Act gives individuals the statutory right to access information held by public authorities — including Government departments and schools — in England, Wales and Northern Ireland.

Data Controller

The data controller is the person or organisation who holds personal data. The Data Controller for The Heights Free School is the Business Manager, Helen Rawnsley.

She will decide why and how any personal data is to be processed and ensure that processing complies with the Data Protection Act 1998.

Other educational bodies such as the Department for Children, Schools and Families (DCSF) and Qualifications and Curriculum Authority (QCA) hold information about individuals for specific functions and they each have a data protection officer.

Data Protection Principles

The data controller must ensure that processing complies with the eight data protection principles, as follows.

1. Personal data must be processed fairly and lawfully. This means:
    - the individual has given consent

- the processing is necessary for a contract that involves the individual, or
- the processing is necessary to comply with a legal obligation, to protect the vital interest of the individual, for legal/justice reasons, or for the purposes of the organisation's legitimate interests.

2. Personal data must only be obtained and processed for specified, lawful purposes.
3. Personal data must be adequate, relevant and not excessive in relation to the specified purpose.
4. Personal data must be accurate and kept up to date.
5. Personal data must not be kept for longer than is necessary.
6. Personal data must only be processed in accordance with the individual's legal rights.
7. Appropriate technical and organisational measures must be taken to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.
8. Personal data must not be transferred outside the EU unless an adequate level of protection for the rights and freedom of the individual is ensured.

Checking Data

The data controller should identify all the information held about staff and pupils, whether held centrally or by individual members of staff. The next step is to consider why and how the data is being kept and measure this against the eight data protection principles. This includes checking that data is accurate, that any irrelevant or excessive personal data is eliminated and that data is only held on a need-to-know basis.

Security Measures

It is important that the data controller puts in place physical and electronic safeguards to protect all data. This means taking measures such as:

- fixing locks to filing cabinets
- fixing locks to doors, to offices, filing rooms and computer rooms
- securely managing the holding and storage of keys
- physically securing computers and servers
- installing anti-virus software
- installing firewall software or hardware
- securing data backup procedures
- following good practice relating to passwords, clear screens, etc
- separating administrative and teaching computer systems.

The degree of security will depend on the means of storage/processing, the nature of the data, the potential for harm and cost.

Once the procedures are set up, managers and staff who process information should be made aware of their responsibilities, amending their practices and retraining if necessary. Staff and pupils and their parents should be told what the establishment's data protection policy is. A fair processing notice is sent out to parents on an annual basis by the Headteacher, a copy of the notice is displayed on the School website.

Personal Data

Personal data covered by the Act may include:

- school admission and attendance registers
- pupils' curricular records

- assessment data under the assessment arrangements of the National Curriculum
- reports to parents on the achievements of their children
- records in connection with pupils entered for prescribed public examinations
- staff records, including payroll records
- pupil disciplinary records
- personal information for teaching purposes
- records of contractors and suppliers.

Sensitive Data

The data controller should ensure that the holding and processing of sensitive personal data complies with at least one legal condition set out in the Data Protection Act 1998.

Sensitive data includes:

- ethnic or racial origin
- political opinions
- religious beliefs
- other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life
- offence or alleged offence
- proceedings or court sentence.

Sensitive data can only be processed if the information has been obtained lawfully and fairly and the subject has consented, with certain exceptions including equal opportunities monitoring.

Disclosure of Data

In general, personal data cannot be released to third parties without the individual's consent, unless for specific reasons such as the prevention or detection of crime, the health, safety and welfare of employees or where the disclosure is to protect the vital interests of the individual. Ideally, the individual's consent should be obtained in writing. Where the data controller wishes to obtain personal data from a third party (eg an employee’s medical records), the individual’s permission should be requested and obtained.

There are certain circumstances when personal data can be disclosed without the individual’s consent, including where the disclosure is:

- necessary for the prevention or detection of crime or collection of taxes or duties
- legally required
- required by a court order or is connected with legal proceedings
- to prevent known harm to a third party, which could occur if data was not disclosed.

All requests for disclosure should be written on headed notepaper and give full reasons.

The School must give accurate information when supplying a reference for an employee or ex-employee.

Access to Data

A system should be created to ensure that requests for access to data can be readily granted. The request for access should be made in writing and describe the information to which access is required. If practicable and reasonable, the information can be copied or printed and posted to the person making the request. Alternatively, arrangements can be made for the individual to view the information.

Employers should explain that access to certain types of information is restricted, eg information about or provided by a third party.

Rights of Individuals

Individuals about whom personal data is held have a number of rights. These include the following.

- When individuals request it, the data controller should tell them whether personal data is being processed, give them a description, and say why it is being processed and to whom the information is being disclosed. The data controller only has to supply staff with their personal data after a request has been made in writing and a fee of not more than £10 has been paid (on request). The data must be supplied within 40 days.
- The data must be communicated in an intelligible form.
- The data must be accurate.
- Information should not be used for a purpose different from the one it was gathered for.
- Job applicants should be told about automated decision-making if this is the only basis for the decision to reject their application.
- Personal information given in confidence must not be disclosed without consent.
- Employees should not be the subject of surveillance or monitoring without good cause, and any surveillance has to be proportionate.

Individuals also have the right to:

- prevent processing which is damaging or distressing to themselves or others
- prevent processing for direct marketing
- ensure that no decision significantly affecting them is based solely on the automatic (electronic) processing of data relating to them, eg assessing their performance at work
- be compensated if they suffer damage and distress as a result of a data controller's contravention of the Act, unless reasonable care to comply with the Act can be proved
- rectify, block, erase or destroy inaccurate data on application to the court
- request that the Information Commissioner assess whether or not the processing of personal data is being carried out in accordance with the Act.

Exemptions

There are many exemptions to the Act. Individuals are not entitled to have access to the following.

- References given by an employer, although it is good practice for employees to be shown references when written.
- Personal data processed for the purposes of management planning, eg pay reviews or promotion opportunities.
- Information about or provided by a third party where the third party could be identified and does not agree to a disclosure.
- A candidate's personal data recorded during an examination or to see their examination marks until the results have been released.

The Act provides for Regulations to be introduced that will mean individuals may not have access to personal data:

- about their physical or mental health — the Access to Medical Reports Act 1988 gives individuals access to any medical report on them supplied by a GP for employment purposes
- about present or past pupils of a school of which the data controller is the proprietor, governing body or Head
- processed by government departments, local authorities (LAs) or voluntary organisations for social work in relation to the individual or others.

Pupil Records and Reports

The keeping, disclosure and transfer of pupil records must take account of the Data Protection Act 1998.

All pupils as well as parents are entitled to have their records disclosed to them on written request, unless it is obvious they do not understand what they are asking for, or if disclosure would be likely to cause them or anyone else serious physical or mental harm. This right is no longer related to the age of the pupil.

When a pupil transfers school, Heads must send to the new school (maintained or independent) a completed statutory transfer form and all educational records relating to the pupil, including copies of their pupil reports.

There is more information in DCSF Guidance 0015/2000 Pupil records and reports and in DCSF Guidance 002/2002 Guidance on the collection and recording of data on pupils' ethnic backgrounds.

Monitoring Staff and Students

Before monitoring staff telephone use, Internet use or e-mails (or installing CCTV cameras) the Data Protection Code of Practice suggests that employers carry out an impact assessment, balancing the needs to monitor against the impact on staff and pupils.

Employers should be clear about the purpose of monitoring and tell employees and students the nature, extent and reasons for any monitoring.

Access to the information gathered should be limited and those with access trained on their responsibilities.

Third parties should be warned if they are likely to be caught by the monitoring.

Covert monitoring should only be carried out in exceptional circumstances and limited to specific investigations where criminal activity or equivalent malpractice is suspected.

List of Relevant Legislation

- Data Protection (Subject Access Modification) (Education) Order 2000
- Education (School Records) Regulations 1989
- Freedom of Information Act 2000
- Data Protection Act 1998
- Human Rights Act 1998
- Access to Medical Reports Act 1988
- Regulation of Investigatory Powers Act

Further Information
Publications

- Equal Pay Review, Equal Opportunities Commission (EOC)
- Employment Practices Data Protection Code — Part 1: Recruitment and Selection, from the Information Commissioner's Office
- Employment Practices Data Protection Code — Part 2: Employment Records, from the Information Commissioner's Office
- Employment Practices Data Protection Code — Part 3: Monitoring at Work, from the Information Commissioner's Office
- The Employment Practices Code — Supplementary Guidance, from the Information Commissioner's Office, 2005
- Responding to an Equal Pay Questionnaire and Requests for Information During Tribunal Procedures in Accordance with Data Protection Act Principles, Equal Opportunities Commission (EOC)
- Circular 15/00 Pupil Records and Reports, Department for Children, Schools and Families (DCSF)

- Guidance on the Collection and Recording of Data on Pupils' Ethnic Background, Department for Children, Schools and Families (DCSF)
- Guidance on the Use of Biometric Systems in Schools, Becta

Organisations

- Advisory Conciliation and Arbitration Service
- Commission for Racial Equality

  Web: www.cre.gov.uk

  The Commission for Racial Equality was a publicly funded, non-governmental body set up under the Race Relations Act 1976 to tackle racial discrimination and promote racial equality. Since 1 October 2007 this organisation has been replaced by the Equality and Human Rights Commission.
- Criminal Records Bureau (CRB)

  Web: www.crb.gov.uk

  The CRB — an executive agency of the Home Office — is set up to help organisations make safer recruitment decisions.
- Equal Opportunities Commission

  Web: www.eoc.org.uk

  An agency which worked to eliminate sex discrimination and put equality into practice in the workplace. Since October 2007, this organisation has been replaced by the Equality and Human Rights Commission.
- Health and Safety Executive (HSE)

  Web: www.hse.gov.uk

  The HSE is responsible for the regulation of almost all the risks to health and safety arising from work activity in the UK.
- Information Commissioner’s Office (ICO)

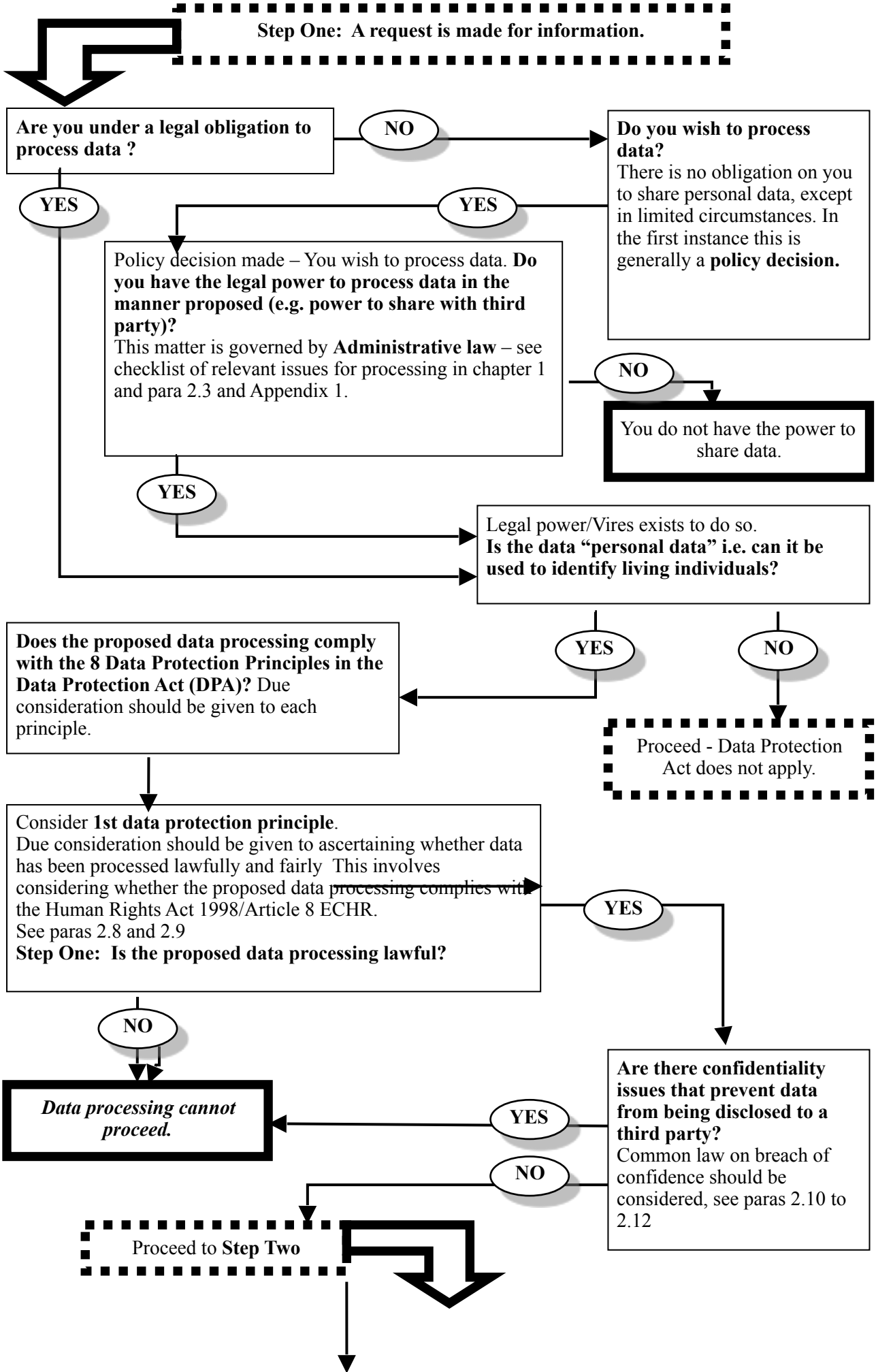
  Web: www.ico.gov.uk

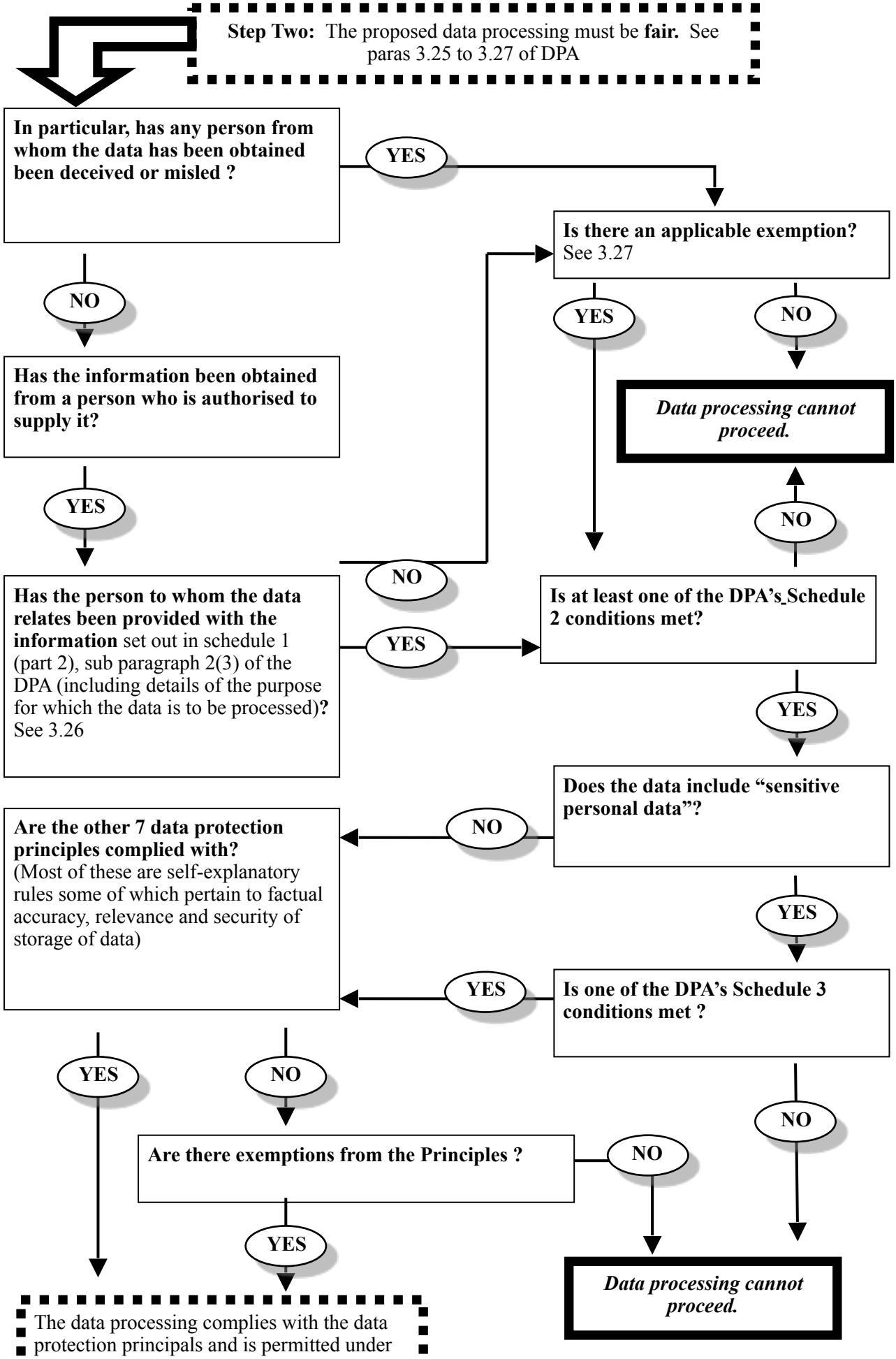
  The ICO enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000. It is an independent UK supervisory authority, reporting directly to the UK Parliament. It has an international role as well as a national one.

ROAD MAP AND CHECKLIST

The road map and checklist provided below are intended to be helpful summaries of the issues to consider when processing personal data. They are not, in themselves, detailed explanations of the law and the relevant chapters of this guidance should be read to acquire a greater understanding of the issues.

Road map of basic process for decision making when processing personal data




Step Two: The proposed data processing must be fair. See paras 3.25 to 3.27 of DPA
In particular, has any person from whom the data has been obtained been deceived or misled ?
YES
Is there an applicable exemption? See 3.27
NO
YES
NO
Has the information been obtained from a person who is authorised to supply it?
Data processing cannot proceed.
YES
NO
NO
Has the person to whom the data relates been provided with the information set out in schedule 1 (part 2), sub paragraph 2(3) of the DPA (including details of the purpose for which the data is to be processed)? See 3.26
YES
Is at least one of the DPA's Schedule 2 conditions met?
YES
Does the data include "sensitive personal data"?
NO
Are the other 7 data protection principles complied with? (Most of these are self-explanatory rules some of which pertain to factual accuracy, relevance and security of storage of data)
YES
YES
Is one of the DPA's Schedule 3 conditions met ?
YES
NO
NO
Are there exemptions from the Principles ?
NO
YES
Data processing cannot proceed.
The data processing complies with the data protection principals and is permitted under the DPA.

Basic process for decision-making on data processing
(where there is no legal obligation to process/share data)

Policy decision
Do you wish to process / share personal data ?

⇩

Do you have the power to process the data
in the manner proposed (or share it with the person / body in question)?

⇩

Does the proposed data processing comply with
the Data Protection Act 1998 ?

⇩

Does the proposed data processing comply with
the Human Rights Act 1998 / Article 8 ECHR ?

⇩

Are there confidentiality issues

that prevent the data from being disclosed to a third party

Data Protection - Advice to staff

Rationale

As a school we hold and process a variety of personal data about staff, students and their relatives. Should this data fall into the wrong hands, it is possible that it may be used to cause harm. We have therefore an ethical, and legal, obligation to ensure that such data is held securely. There may be times, however, when it is necessary to take data out of school (e.g. student marksheets to record assessments).

What do we mean be "data"?

It may be helpful to divide such data into two broad categories:-

1. **High Risk Data**, with a high potential for harm, e.g. contact information (addresses, phone numbers), employment details (bank details, NI numbers etc), medical records, IEP's, user names and passwords, external exam results and photographs from which individuals may be identified. *(Equivalent to Becta Impact Level 3 & 4)*
2. **Low Risk Data**, with a very low potential for harm, e.g. lists of student names, internal assessment grades, photographs that are unidentified. *(Equivalent to Becta Impact Level 2)*

What data should leave the school?

It is the responsibility of all staff to ensure that **all data**, whether "high" or "low" risk, is held securely at all times. However, **it is the general rule that only "low risk data" should ever leave the school**. Any exceptions to this rule are dealt with individually below.

Possible ways that data might accidentally leave the school

Paper-based records (mark books, class lists etc)
Memory sticks
Email
Laptops
Web portal
CD/DVD
Portable hard drives

Exceptions to the rule

1. Staff organising and running trips etc may need to take contact details off site in case emergencies arise. In this case:-

- Only paper copies should leave the school. Electronic copies on memory sticks, laptops, email etc should under no circumstances leave the school.
- The number of paper copies made should be strictly controlled and a record kept by the event leader of who holds one.
- After the trip etc is over, the event leader is responsible for collecting back in each copy and seeing that they are securely destroyed in school.
- If any data is unaccounted for, this must be reported immediately to the SLT link (WG).

2. Staff use of the Management Information system – please refer closely to separate instructions provided for its use.
Please refer to IT support for advice on the secure transmission of data. **NB** email is inherently insecure and should never be used to send "high risk data" either to or from school.

If any member of staff wishes to take "high risk data" out of school under other circumstances, they should first clear this with the SLT link to ensure that this complies with the school's Data Protection policy. A record of this data will be kept centrally.

Use of the internet in school

Although students are limited in what they can access on the internet by web filtering, it is still the responsibility of teaching staff to closely monitor the websites visited during lessons. Proxy servers are commonly used to bypass web filtering.

If a student cannot log on in their own name, check that they are not banned from the internet. If so, alternative work must be found for them. **Under no circumstances should the student be allowed to use the member of staff's log on.** This would allow the student unauthorised access to "high risk data", e.g. staff home phone numbers etc.

Advice relating to Social Networking sites

Although social networking sites such as Facebook, Twitter and YouTube are a great way to meet new people and discuss shared interests it is still important that staff in school remain safe even whilst online.

Local Authorities and other public sector agencies are increasingly looking to social media to engage with their audiences as a more efficient way of bringing people together, consulting people and obtaining feedback.

However, they should be treated with respect as there can be a number of risks associated with social networking for a school such as damage to its reputation, disclosure of confidential information and potential vicarious liability for any discriminatory behaviour or cyber-bullying. Any information or comments published on any site (internal or external)

- May stay in the public domain for a long time
- Can be republished on other websites
- Can be copied, used and amended by others
- Could be changed to misrepresent what was said
- Can attract comments and interest from other people/the media

The guidance below should help you to manage any issues that arise

Using social media

Nearly all social network websites allow an individual to control who can see their information and therefore it is advisable that staff take the time to look over the privacy settings.

Colleagues and pupils may see their online information therefore encourage staff that whether or not they identify themselves as an employee of a school they need to think carefully about how much information they want to make public and make sure any information they post is professional as they are personally liable. They should never give out personal details like home addresses, phone numbers, financial information or full date of birth to prevent identity theft.

Employees need to be aware that whilst at school the internet is used primarily for business use and that whilst the school does allow access to social networking websites from its computers this should be done before and after work and during break times if it is not work related and in line with the school acceptable use of IT Policy; and as such fair use, financial disclosure, libel defamation, copyright and data protection laws apply on-line just as in any other media.

Keeping it private and decent

Employers should consider their obligations to pupils, partners and colleagues and to protecting the school's reputation when using such sites. They should never give out details of colleagues, customers or partners without prior consent and should never make offensive comments, ethnic slurs, personal insults, obscenity or behave in ways that are not acceptable in the workplace. This could bring the school into disrepute and leave the employee open to prosecution and/or disciplinary action.

It is not a good idea or recommended to invite pupils to become friends on social networking sites as there may be a conflict of interest. Entries, articles or comments should be of a neutral tone, factual and truthful and rude or offensive comments should never be posted.

Speaking for the school

Employees should be informed not to speak for the school, disclose information, make commitments or engage in activities on behalf of the school unless authorised to do so.

Giving personal views

Employees should be reminded of the requirements to remain professional as they will be seen as representing the school if people become aware of their links, even if not speaking on the school's behalf. In these instances staff should make it clear that they are speaking for themselves and not on behalf of the school or Local Authority, if such information is published on a website this must include a simple disclaimer such as "The views expressed here are my own and don't necessarily represent the view of …. eg Eden School."

Employees should also be aware that these things may attract media interest and that if contacted they should take contact details and take appropriate internal advice before responding. Any concerns should be discussed with the individual's line manager.

Please make sure that staff are aware of and working within these guidelines. If you believe any employee is breaching these guidelines or if you require any clarification regarding the above material or need further advice and guidance please do not hesitate to contact the chair of Governors.