Futura Learning Partnership

Children • Choice • Collaboration

Data Protection Handbook

Contents

Contents 1

Data Protection Policy.....6

1. Aims 6

2. Scope 6

3. Distribution.....6

4. Definitions.....6

5. Roles and Responsibilities.....8

6. Data Protection Officer 9

7. Data Subject Rights.....9

7.1 The Right to be informed 9

7.2 The Right of access.....9

7.3 The Right to rectification.....10

7.4 Right to erasure.....10

7.5 The Right to restrict processing 10

7.6 The Right to data portability.....10

7.7 The Right to object.....11

8.Data Protection Principles 11

9. Processing Personal Data 13

9.1 Processing Special Categories of Personal Data 13

9.2 Legal basis for processing criminal offence data 14

10. Third Parties with Access to Personal Data.....15

10.1 Data Sharing 15
10.2 Third-Party Processors 15
10. Data Protection by Design and Default 16
11. Data Protection by Design and Default 16
12. Personal data breaches or near misses 16
13. Biometric Recognition Systems 16
14. Destruction of records 17
15. Training 17
16. Monitoring Arrangements 17
17. Complaints 18
18.Legislation and Guidance 18
19. Links with Other Policies 18
Appendix 1 – Examples of Special Category Data that we process 19
Appendix 2 – Subject Access Request Procedure (SAR) 20
Information Security Policy 21
20. Introduction 21
21. Scope 21
22. Aim 21
23. Roles and Responsibilities 22
23.1 Information Security Lead 22
23.2 Data Protection Officer (DPO) 23
23.3 Managers/Senior Staff 23
23.4 Head of IT/IT Lead 23
23.5 Information Owners/Responsible Persons 24
23.6 All Employees and External Individuals 24
24. Areas That Require Specific Adoption of Information Security 25
24.1 Contracts of Employment 25
24.2 Control of Information Access 25
24.3 Staff Owned Devices 25
24.4 Computer Access Controls 25
24.5 Application Access Controls 26
24.6 Equipment Security 26
24.7 Computer Network Procedures 26

24.8 Information Security Breaches and Reporting....26
24.9 Protection from Malicious Software....26
24.10 Removable Media....27
24.11 Monitoring System Access and Use....27
24.12 Accreditation and Assessment of Systems....27
24.13 System Control Change....27
24.14 Business Continuity and Disaster Recovery Plans....27
24.15 Training and Awareness....28
25. Document Classification....28
26. Associated Policy and Guidance....30
Data Protection Impact Assessments....31
27. Definitions....31
28. Background information....32
30. Duties and responsibilities....32
31. The benefits of a DPIA....33
32. The DPIA process – key points....33
33. Guidance for completion of a DPIA....34
34. Appendices....36
Appendix 3 – Potential privacy risks....37
Appendix 4 – Useful links....39
Appendix 5 – Overview of the DPIA process....40
Appendix 6 – DPIA template....41
Data Breach Policy....53
35. Introduction....53
36. Scope....53
37. Data Breaches....53
38. Risk Assessment and Reporting....54
39. Monitoring and Compliance....55
40. Links with Other Policies....55
Appendix 7 – Data Breach Reporting Form....56
Records Management Policy....58
41. Introduction....58
42. Objectives....58

43. Definitions....58
44. Scope....58
45. Responsibilities....59
46. Creation & Storage....59
47. Retention and Disposal....59
47.1 Retention Schedule....60
47.2 Definition of Retention Periods....60
47.3 Reviewing Retention Periods....61
47.4 Course of Action at the End of the Retention Period....61
47.5 Disposal....61
47.6 Archiving....62
47.7 Protective Marking....62
48. Monitoring and Compliance....62
49. Relationship with Existing Policies....62
Appendix 8- What is Confidential Waste?....62
Appendix 9- Retention Schedule....64
Governance and School Management....64
Human Resources....71
Financial management of the trust....76
Property Management....80
Pupil Management....82
Curriculum Management....86
Extra-Curricular Activities....88
Central Government and Local Authority....91
Appendix 10 - Quick Calculators....93
Quick calculator - ACADEMIC YEARS - DISPOSAL BY 31.08.23....93
Quick calculator- CALENDAR YEARS - DISPOSAL BY 31.12.23....94
Quick calculator- FIXED PERIOD....95

Welcome

This new Handbook has been developed to bring together all Data Protection Policies into one handbook and includes:

- Data Protection Policy – this is the primary policy in this suite of policies and details how you should protect data, together with how and who it can be shared with. There are sections on the rights of individuals to ask to see or have data removed.
- Information Security Policy – this details how you should be ensuring the security of data that you hold.
- Data Protection Impact Assessment Policy – this details the process which should be used to assist the school in identifying, minimising and addressing the privacy risks associated with any new initiative.
- Data Breach Policy – this details the process you should follow should there be a data breach in your school/office/etc.
- Record Management Policy – this details what documents must be retained, for how long and how they should be disposed of after the retention period.

We acknowledge that it is a weighty document, but hope that it will save you time in ensuring you have everything you need in one place. If you have any ideas on how this could be improved to make in even more user-friendly, please feedback to the Director of Business and Operations.

Data Protection Policy

1. Aims

The Executive Leadership Group (ELG) and Trustees of Futura Learning Partnership are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Futura Learning Partnership are registered as a data controller with the Information Commissioner.

The details of the Futura Learning Partnership's Data Protection Officer can be found at paragraph 6.

2. Scope

This policy applies to anyone who has access to data and/or is a user of Futura Learning Partnership's ICT systems, both in and out of Futura Learning Partnership, including staff, Trustees, volunteers, visitors, contractors, and other community users.

This policy is also intended to serve as the appropriate policy document for the processing of Special Category Data and Criminal Record Data (where applicable).

This policy applies to all personal data for which Futura Learning Partnership is the Data Controller, regardless of whether it is in paper or electronic format.

3. Distribution

This policy is available on the Futura Learning Partnership website and in hard copy from the Futura Learning Partnership school offices.

4. Definitions

Personal data - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. We may process a wide range of personal data of staff (including Trustees, Governors and volunteers) and residents as part of its operation. A non-exhaustive list of examples of the types of personal data that we process can be found in our Privacy Notices.

Special category personal data - Formerly known as "sensitive personal data", Special Category Data is information that might not necessarily identify a person, but is a lot more sensitive to that person. These are:

- racial or ethnic origin
- political opinions
- religious / philosophical beliefs

- trade union membership
- genetic data
- biometric data (for identification purposes)
- health data (mental and physical)
- sex life or sexual orientation

Examples of the types of special category data we process can be found at Appendix 1. Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as do our Privacy Notices which can be found on our website.

Data Subject(s) - The Data Subject is the person about whom the personal data relates or identifies.

Data Processing - Data Processing is an over-arching term that means "doing something" with personal data. This commonly includes:

- Collecting or collating the data
- Analysing the data
- Sharing the data
- Storing the data
- Destroying the data

Data Controller - The Data Controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that organisation undertakes. They will make all the decisions about what is captured, how it's used and the purpose for it, as well as deciding what controls need to be in place.

Data Processor - is occasionally a person, but more commonly an organisation commissioned by a Data Controller to carry out their data processing on behalf of the Data Controller. These are usually software providers such as Microsoft, or contracted out services such as an insurance company. Essentially, a Data Processor is acting as an extension of the Data Controller, so must operate under the Data Controller's instructions, and under the terms of a Data Processing Agreement.

Data Sharing - means *giving* it to another Data Controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the Data Controller for that information, and therefore makes the decisions over what they will do with it.

Note, we do NOT *share* data with our Data Processors, as these are processing it under our Data Controllership.

Data Breach - The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example sending an email to the wrong recipient, losing a file containing personal data, or sharing passwords enabling someone else to access your account. However, we consider any failing of one of the Data Protection Principles (Article 5 of UK GDPR) as a breach of data protection legislation, so could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of UK GDPR).

Data Processing Agreement – a legally binding contract between the Data Controller and its Data Processor. This contract defines exactly how the Data Controller expects the Data Processor to process its personal data, and follow standard contract clauses.

Data Sharing Agreement - a non-legally binding written agreement between Data Controllers where there is regular sharing of personal data. The Sharing Agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, the how the data will be shared.

5. Roles and Responsibilities

Futura Learning Partnership's Trustees have overall responsibility for ensuring that Futura Learning Partnership and its schools comply with all relevant data protection obligations.

Data Protection Lead – each school and the central Team must nominate at least one named person who will act with the delegated authority of the Trustees on a day-to-day basis and will liaise with the DPO. In their absence, in case of emergency, this role will be delegated to the headteacher or Deputy Head.

All other staff (as defined in scope) - All staff are responsible for:

- Familiarising themselves with and complying with this and related policies. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by Futura Learning Partnership for accessing and processing personal data, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data; and locking devices when they are temporarily left unattended at any point (Windows Button + L is a handy shortcut);
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices
- Deleting any data they hold in line with this policy, the Records Management Policy, and the retention schedule;
- Informing Futura Learning Partnership of any changes to their personal data, such as a change of address;
- Reporting to the Data Protection Lead in the following circumstances:
  - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
  - If they have any concerns that this policy is not being followed;

- If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
- If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
- The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and section 12 of this policy;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required and potentially a data protection impact assessment, please see - *Sharing Personal Data* (section 10).

6. Data Protection Officer

Data Protection Officer (DPO)The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance to the organisation and, where relevant, provide the organisation with advice and recommendations on data protection issues.

Futura Learning Partnership has appointed One West as its DPO, and they can be contacted by email at:

One West (Bath and North-East Somerset Council)	Email: i-west@bathnes.gov.uk
Guildhall, High Street, Bath, BA1 5AW	Telephone: 01225 395959

Under usual circumstances the Data Protection Lead will be the point of contact with the DPO.

7. Data Subject Rights

In all aspects of its work, the organisation will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of our work. Subject to exceptions, the rights of the data subject as defined in law are:

7.1 The Right to be informed

We advise individuals how we will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

7.2 The Right of access

An individual when making a subject access request (SAR) is entitled to the following;

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

We must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by up to a further two calendar months. Please refer to Appendix 2 of this policy for further details as to how to manage a subject access request.

7.3 The Right to rectification

Individuals have the right to ask us to correct information they think is inaccurate or incomplete. We have a duty to investigate any such claims and rectify the information where appropriate within one calendar month, unless an extension of up to a further two calendar months can be justified.

7.4 Right to erasure

Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

- The information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- The information is no longer required;
- The data was collected from a child for an online service; or
- We have processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of Futura Learning Partnership to continue to process it.

We will consider such requests as soon as possible and within one month, unless it is necessary to extend that timeframe for a further two months on the basis of the complexity of the request or a number of requests have been received from the individual.

7.5 The Right to restrict processing

This is not an absolute right. An individual may ask us to temporarily limit the use of their data (for example, storing it but not using it) when it is considering:

- A challenge made to the accuracy of their data, or
- An objection to the use of their data.

An individual may also ask us to restrict the destruction of a record, if they wish it to be retained beyond the normal retention period.

In addition, we may be asked to limit the use of data rather than delete it:

- If the individual does not want Futura Learning Partnership to delete the data but does not wish it to continue to use it;
- In the event that the data was processed without a lawful basis;
- To create, exercise or defend legal claims.

7.6 The Right to data portability

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. We only have to provide the information where it is electronically feasible.

7.7 The Right to object

Individuals have a right to object in relation to the processing of data in respect of:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes
- a task carried out for the exercise of official authority
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

Only the right to object to direct marketing is absolute, other objections will be assessed in accordance with data protection principles. We will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress.

8.Data Protection Principles

Data protection legislation is based on seven key data protection principles that Futura Learning Partnership complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – we will explain to individuals why we need their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). We review our documentation and the basis for processing data on a regular basis
- **Collected for specified, explicit and legitimate purposes** – we explain these reasons to the individuals concerned when it first collects their data. If we wish to use personal data for reasons other than those given when the data was first obtained, we will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. In which case, we will document the basis for processing.
- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** we must only process the minimum amount of personal data that is necessary in order to undertake our work.
- **Accurate and, where necessary, kept up to date** – we will check the details of individuals on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- **Kept for no longer than is necessary for the purposes for which it is processed** – we review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When we no longer need the personal data it holds, we will ensure that it is deleted or anonymised in accordance with the retention schedule. We only keep personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;

- We have a retention and disposal/records management policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
- Once the data is no longer needed, we delete it, securely destroy it in line with our retention and disposal policy, or render it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – Futura Learning Partnership implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy and Staff Acceptable Usage Policy (held within the Online Safety Policy for further information which incorporates principles around Bringing Your own Device (BYOD) and how data is securely transferred in and out of our systems.
  - We adopt a risk- based approach to taking data offsite. Unless absolutely necessary, hard copies of special category personal data will not be removed from our premises.
  - Any decision to remove the information must be based on the business need of the organisation or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any special category personal data to be accessed via an appropriately encrypted means rather than via hard copy, when off-site.
  - If there is no reasonable alternative to removing hard copies from the organisation name's site, the following procedure will apply:

i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data in trip packs;

ii. Information will be transported and stored on a lockable electronic device;

iii. We adopt a risk- based approach, for example hard copy personal data with lower sensitivity (e.g. notebooks) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special Category Data (e.g. SEND, Safeguarding, Health data) must be kept on the staff member's person at all times.

iv. Special category data must be returned to our premises at the end of the working day. If this is not practicable, and a staff member needs to retain the information in their personal possession, this must be discussed in advance with a member of SLT including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the SLT must record their decision.

v. Data will be tidied away when not in use (e.g. when staff undertake working at home, it must be out of sight of family members, not left out and tidied away afterwards).

vi. Only those who have need to access the data concerned will be granted permission and access to it.

vii. Our online safety policy / data security policy / acceptable use / remote working policies describe the requirements around bring your own device, remote working and password protection.

- **Accountability –** Futura Learning Partnership complies with its obligations under data protection laws including the UK GDPR and can demonstrate this via the measures set out in this policy including completing Data Protection Impact Assessments (DPIAs) where necessary and sharing them with the Compliance Officer; integrating data protection into internal documents including this policy, any related policies and Privacy Notices; regularly training members of staff on all

relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance using the annual compliance statement and / or Risk Register.

9. Processing Personal Data

In order to ensure that Futura Learning Partnership's processing of personal data is lawful; we will always identify one of the following six grounds for processing **before** starting the processing:

- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent. We will seek consent (where appropriate) to process data from the individual or parent, depending on their mental capacity to understand what is being asked for.
- The data needs to be processed so that we can fulfil a **contract** with the individual, or the individual has asked us to take specific steps before entering into a contract;
- The data needs to be processed so that we can comply with a **legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual, i.e. to protect someone's life;
- The data needs to be processed so that we, as a public authority, can **perform a task in the public interest, or carry out its official functions**;
- The data needs to be processed for our **legitimate interests** or those of a third party where necessary, balancing the rights of freedoms of the individual. However, where we can use the public task basis for processing, we will do so rather than rely on legitimate interests as the basis for processing.

9.1 Processing Special Categories of Personal Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the UK GDPR. The grounds that we may rely on include:

a) The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment and social security and social protection law and research***; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.

c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent;

d) Processing is carried out in the course of its legitimate activities by a **not-for-profit organisation** with a political, philosophical, religious, or trade union aim on the condition that the processing relates solely to its members, or former member who have regular contact with it, and that the personal data are not disclosed outside that body without consent.

e) Processing relates to personal data which are **manifestly made public** by the individual;

f) Processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity;

g) Processing is necessary for reasons of **substantial public interest*** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision- making process.

These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

h) Processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of **health or social care** or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) Processing is necessary for reasons of **public interest in the area of public health*;**

j) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

* We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest.

9.2 Legal basis for processing criminal offence data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

We do not maintain a register of criminal convictions.

When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection;
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual;
- The processing is necessary for statutory purposes; or

- Consent – where freely given. We acknowledge because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other grounds apply.

10. Third Parties with Access to Personal Data

Please refer to our Privacy Notices for details of who, aside from Futura Learning Partnership, has access to the personal data processed.

10.1 Data Sharing

Futura Learning Partnership will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

- We will share data if there is an issue with an individual or parent/carer that puts the safety of staff or others at risk;
- We will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing." In limited circumstances, data may be shared with external agencies without the knowledge or consent of the parent or child in line with the DPA 2018, which includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent;

We may also disclose personal data to law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:

- For the prevention or detection of crime and/or fraud;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided or it is otherwise fair and lawful to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects staff, Trustees or Governors.

10.2 Third-Party Processors

Futura Learning Partnership's suppliers and contractors, including its Data Protection Officer and IT provider, may need access to data to provide services. When third parties are processing personal data on behalf of us, we will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data it shares where there is regular sharing;
- Only provide access to data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working.

11. Data Protection by Design and Default

Futura Learning Partnership has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity, One West must be consulted and an initial screening be conducted assessing risk.

Please refer to the Information Security Policy for further detail as to how we implement this principle in practice.

12. Personal data breaches or near misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred, or a "near-miss" has occurred, the staff member must inform the Data Protection Lead and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy (Section 20).

13. Biometric Recognition Systems

Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form of fingerprint, voice, or facial recognition. We use biometric for example cashless catering, library systems or door entry.

We will undertake a Data Protection Impact Assessment before implementing any new biometric system to assess the impact on individuals.

In the case of adults, for example staff members, we will seek their consent direct from them before processing any biometric data.

In accordance with the Protection of Freedoms Act 2012, in the case of children, we will notify all those will parental responsibility in the case of any individual under 18, unless this is impractical (for example the whereabouts of the parent is unknown or if there is a safeguarding issue) and may only proceed if we have at least one positive written consent, and no written

parental objection. We will not proceed to process the information if the child themselves objects. Either parents or the child may withdraw their consent at any time.

If the individual concerned does not agree to proceed or wishes to withdraw their consent to the use of the biometric system, we will provide an alternative means of achieving the same aim.

14. Destruction of records

We adhere to our retention policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes.

We will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

Where we delete electronic records and its intention is to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

15. Training

To meet its obligations under Data Protection legislation, we will ensure that all staff, volunteers, and Governors / Trustees receive an appropriate level of data protection training as part of their induction. Permanent members of staff will receive Data Protection training at least every 2 years. Those who have a need for additional training will be provided with it, for example relating to use of systems or CCTV or if they regularly deal with sensitive data.

Data protection also forms part of continuing professional development. Staff members undertake regular informal discussions on Data Protection, to ensure key updates are provided where changes to legislation, guidance or our processes make it necessary. This will include lessons learned from Data Breaches and Near Misses, preventative measures to avoid them, and other best practice as advised.

16. Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring Futura Learning Partnership's overall compliance with data protection law, we are responsible for the day-to-day implementation of the policy and for making the data protection officer aware of relevant issues which may affect our ability to comply with this policy and the legislation.

This policy will be reviewed annually, unless an incident or change to regulations dictates a sooner review.

17. Complaints

Futura Learning Partnership is always seeking to implement best practice and strives for the highest standards. We operate an "open door" policy to discuss any concerns about the implementation of this policy or related issues. Our complaints policy can be found on our website.

There is a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the organisation or via the our DPO.

The ICO is contactable at:

www.ico.org.uk

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113

18.Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Information Sharing – Advice for Practitioners – DfE July 2018.

19. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Retention & Disposal / Records Management Policy
- Data Breach Policy
- Privacy Notices
- Child Protection and Safeguarding Policy

- Online Safety/Acceptable Usage Policies
- Consent / Permissions Form
- Admissions Form
- CCTV
- IT Security Policy

Appendix 1 – Examples of Special Category Data that we process

Examples of where we may process special category data include in:

Employee health data and information concerning their racial / ethnic origin

Pupil health data and information concerning their racial / ethnic origin in admissions records and in pupil records / trip packs

Special Educational Needs information

School census information

Attendance records

Biometric data i.e., fingerprints for cashless catering / door entry systems

Information contained within child protection and safeguarding records

Staff / Governor/ Trustee application forms

HR / payroll files including and disciplinary and capability proceedings which may include DBS, and right to work checks, health, and equal opportunities data (disability, race, ethnicity, sexual orientation).

Accident reporting documentation

Trustee and governor health data and information concerning their racial / ethnic origin and disabilities

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it; as does our Privacy Notice which can be found on our website.

Appendix 2 – Subject Access Request Procedure (SAR)

Futura Learning Partnership shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (One West).

1. Ascertain whether the requester has a right to access the information and capacity.
2. Obtain (reasonable and proportionate) proof of identity
3. Engage with the requester if the request needs clarifying

   Nb only once steps 2 and 3 have been completed, can the "clock" start
4. Make a judgement on whether the request is complex and therefore can be extended by an additional two months
5. Acknowledge the requester providing them with
   a. the response time – one calendar month (as standard), an additional two months if complex; and
   b. details of any costs – free for standard requests, or you can charge, or refuse to process, if the request is manifestly unfounded or excessive, or further copies of duplicate information is required, the fee must be in line with the administrative cost
6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held
7. Collect the data (the organisation may use its IT support to pull together electronic data sources such as emails and databases)
8. If (6) identifies third parties who process it, then engage with them to release the data to Futura Learning Partnership.
9. Review the identified data for exemptions and redactions in line with the ICO's Guide to the Right of Access and in consultation with the organisation's Data Protection Officer (i-west)
10. Create the final bundle and check to ensure all redactions have been applied.
11. Submit the final bundle to the requester in a secure manner and in the format they have requested.

Information Security Policy

20. Introduction

Futura Learning Partnership is responsible for the control of a number of individuals' Personal Data (PD) including staff, governors, pupils, clients, and a number of other individuals who interact with Organisation name. In addition to PD, information that may be considered of a sensitive nature will include financial records, planning and management forecasts, and risk assessments, which also require appropriate security applications to be made and are included within the scope of this policy.

The Information Security Policy (ISP) is designed to inform employees of the appropriate principles and methods to create, store, secure and, dispose of information in all formats to ensure security is of a consistently high standard. Compliance with this Policy provides management, staff, and associated individuals with:

- Assurance that information is being managed securely in a consistent and effective way.
- Assurance that Futura Learning Partnership is able to provide a trusted environment in which to handle information as part of its activities.
- Clarity regarding the individual responsibilities for Information Security.
- Demonstration of best practice.
- Assurance that information may only be accessed by those authorised to have access.

21. Scope

This policy applies to all employees of Futura Learning Partnership including contract, agency and temporary staff, volunteers and employees of partner organisations working with or for Futura Learning Partnership.

The ISP can be used by employees who use data as part of their day-to-day business, those who manage and administer data and by those responsible for the management of data storage systems.

22. Aim

The ISP aims to ensure that all employees are aware of the following principles of the CIA Triad when dealing with information and use the principles from their day-to-day handling of information up to the development and adoption of new ways and systems designed for handling information. These principles will also help Futura Learning Partnership comply with Article 32 of the UK GDPR which refers to adequate organisational and technical security;

Confidentiality: Information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity: Maintain the accuracy and completeness of data over its lifecycle.

Availability: Information must be available when needed and appropriate means of access or disclosure must be understood.

In addition to the protection and maintenance of the confidentiality, integrity, and access of data this policy will support the organisation to meet the following:

- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Adoption of this concept will reduce the risk of harm to individuals, reduce the vulnerability of the organisation, and the likelihood of financial penalties that may be given by supervisory authorities such as the Information Commissioner's Office (ICO).

23. Roles and Responsibilities

23.1 Information Security Lead - Accountability for Information Security rests with the Information Security lead who is the Headteacher. The Information Security Lead may discharge this function to the Deputy Head or another Responsible individual to carry out the activities of Information Security.

Such activities may include.

- Evaluating and accepting risk on behalf of the trust.
- Identifying information security responsibilities and goals and integrating them into relevant processes.
- Supporting the consistent implementation of information security related policies and processes.
- Supporting security through clear direction and demonstrated commitment of appropriate resources.
- Promoting awareness of information security best practices through the regular dissemination of relevant material such as that provided by the Data Protection Officer (DPO).
- Implementing the process for determining information classification and categorisation, based on recommended practices, and legal and regulatory requirements, and to determine the appropriate levels of protection for that information.
- Implementing the process for information asset identification and recording them in the Record of Processing Activities (RoPA) as well as the handling, use, transmission, and disposal based on information classification and categorisation.
- Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.

- Participating in the response to security incidents.
- Complying with notification requirements in the event of a breach of personal data.
- Adhering to specific legal and regulatory requirements related to information security.
- communicating legal and regulatory requirements to the ISO/designated security representative, specifically Article 32 of the UK GDPR (Security of Processing).
- Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

Governance of Information Security may be formalised to include a regular review and working group to identify business requirements and how they impact existing information use and future use.

23.2 Data Protection Officer (DPO) - The DPO, i-West, is responsible for monitoring the organisation's compliance with Data Protection legislation. This is completed by the following means: an annual assurance review; breach and security incident monitoring; and review and providing sufficient guidance to the Information Security Lead for them to carry out their task where PD may be processed.

The DPO will support the organisation in the event of any breach of information where it relates to personal data.

23.3 Managers/Senior Staff - Primarily responsible for ensuring the security of the systems that hold data and the physical environments where information is processed or stored. They are also responsible for the following:

- Ensuring all employees within their area of work are aware of the relevant polices applicable to their role i.e. Acceptable Use Policy, Confidentiality agreements, Bring Your Own Device (BYOD) guidelines and eSafety.
- Determining and controlling the access levels of employees and relaying that information, including when access must be removed, to the Head of IT or individual responsible for the control of electronic access.
- The control of passwords, keys, combination lock numbers or any other physical form of access control within their area of work.
- Ensuring that employees have taken part in the relevant and adequate training in a timely manner.
- Making employees aware of security breaches or threats and translating points learnt from such incidents into working practices.

23.4 Head of IT/IT Lead - The Head of IT or individual responsible for management of IT whether on-site or through a third-party contract must ensure that.

- All network, mobile devices, and removable media assets are securely controlled and managed. This includes maintaining appropriate storage facilities, producing, and reviewing guidance regarding the safe storage and use of assets, user access agreements and user access control, such as the removal of users when informed to do so by managers, or under exceptional circumstance.

- The maintenance of software in use by the organisation. This includes software patching routines, application or alterations or the removal of software considered to be vulnerable, the assessment of such levels of vulnerability, and the notification to all relevant staff of existing threats, emergent threats, and appropriate safe use. This information may be provided to managers in support of their responsibilities for awareness.
- The development and implementation of new technologies to build safe and secure systems. The direction of this responsibility should be agreed with the Information Security Lead.

23.5 Information Owners/Responsible Persons - The approach to the use of data will determine who Information Owners are. In general, the ownership or responsibility will fall to the relevant manager, or person who retains and uses the information within their workspace, for example the Lead Administrator will own the data used within the School office, including centralised pupil information; the Designated Safeguarding Lead (DSL) will own Safeguarding Information; and individual teachers will own class lists and pupil information where it is not held on the Pupil Information Management System.

It is good practice to record the relevant owner or responsible person so that any issue regarding the use, management or breaches of that information may be brought to their and the DPO's attention. This is referred to as an Information Asset List, however it may be incorporated into the Record of Processing Activities (RoPA) used for Data Protection purposes.

Information Owners will be responsible for managing the accuracy and security of their data. This will mean that their relationship with their peers and managers, where applicable, is key to ensuring the CIA Triad is observed.

Owners will also need to discuss with the Information Security Lead and DPO the implications of using third parties to process information or when sharing information. Where this includes PD or other sensitive information, appropriate agreements must be in place.

23.6 All Employees and External Individuals - Everyone is responsible for Information Security and should be aware of and understand the requirements of on them in line with this Policy and any associated guidance.

The key points for all employees to remember are.

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted to them.
- Protecting information and resources from unauthorised use or disclosure.
- Protecting personal, private, sensitive information from unauthorized use or disclosure.
- Abiding by policy and guidance related to information security such as Online Safety, Acceptable Use, confidentiality agreements and the conditions of use of any device issued by the trust.
- Reporting suspected information security incidents or weaknesses to the appropriate manager.

Individuals who may work in the trust with information but not be an employee, such as IT technicians, auditors or external agencies, should be able to demonstrate their organisation's

Information Security approach or have an appropriate confidentiality statement within their work description.

They should be made aware of what they should do if they inadvertently access information that they should not have done or discover a breach. This may be as simple as letting them know to contact the person who is responsible for them or making them aware of who the relevant manager is that they can report to.

24. Areas That Require Specific Adoption of Information Security

24.1 Contracts of Employment - Staff suitability must be assessed at all points of employment, in line with safer recruitment policies and guidance, and all employee contracts must contain reference to confidentiality. Information in the form of the Acceptable Use Policy, Data Protection Policy or specific confidentiality guidance must be provided to employees at the appropriate time.

24.2 Control of Information Access - Information shall be restricted to only those who have an acceptable business reason to access such information.

Information Owners/Responsible Persons must be consulted before access is granted or an appropriate process of access must be in place.

Passwords or emergency access without authorisation may only be made in exceptional circumstances and the decision to do so must be relayed to the relevant Information Owner, Manager, or the Information Security Lead at the earliest possible point.

24.3 Staff Owned Devices

- Staff must not use their own devices to take images of young people.
- Only trust equipment may be used and images must be deleted as soon as they are no longer required, saved securely on trust systems and deleted in accordance with the retention policy.
- Pass-codes or PINs must be set on personal devices to aid security; and where possible encryption applied to the device.
- Users are expected to act responsibly, safely, and respectfully in line with current Acceptable Use Agreements.
- Users must log out of trust programmes and applications when they are not in use.
- The device must have the latest updates applied.
- Passwords must not be saved, for example to the browser history.
- Users must not download data locally to the device (e.g. email attachments).

24.4 Computer Access Controls - Access to computer systems must be managed by IT or the person responsible for IT. This may be by active directory or, in the case of portable devices, by providing a temporary password.

There must be a form of system monitoring that can be used to determine who accessed which device and at what time, at a basic level this may be using Active Directory, Event Viewer, or a more complex User activity Monitor (UAM) software.

The fundamentals of password security are required to ensure that passwords are not shared which would result in misidentification with the exception of the point regarding emergency access in the previous paragraph.

24.5 Application Access Controls - Specific applications must be administered effectively by either IT or the responsible person for any third-party application, such as but not limited to, Tapestry, Class Dojo. This is particularly relevant for the Pupil Management System; however, this applies to all other applications where it has been deemed that access controls are required.

When adopting a new application, a proper assessment of access controls must be made and, if necessary, locally produced guidelines regarding its use should be made. This may be covered as part of a Data Protection Impact Assessment.

24.6 Equipment Security - Information may be stored in physical containers such as filing cabinets, draws, safes and storage rooms. It will in most cases be retained electronically, however the principles of security are the same.

Any area where information is stored must be secured in a manner appropriate to the type and sensitivity of information stored within, for example sensitive financial records, safeguarding records and HR records must be secured by lock, or if stored electronically on a secure section of the computer network isolated by specific permissions.

General lists and necessary contact details should be stored out of sight in line with a clear desk routine, or, if stored electronically, may be stored in a general open section of the computer network.

Information Owners must assess the level of security required and where necessary consult with the Information Security Lead and Head of IT. In cases where highly sensitive information is stored electronically, it should be encrypted wherever possible.

24.7 Computer Network Procedures - The arrangement and control of the computer network should be documented and must not remain with a single person. The reliance upon a sole individual's understanding of the system can undermine the principle of availability, if they leave or are unavailable, due to the potential loss of access, and may lead to loss of data if a full understanding of the type and location of data is not retained.

24.8 Information Security Breaches and Reporting - Any breaches of information security must be reported to the Information Security Lead and, where it involves the inappropriate access via hacking, malicious attack, lack of security around an electronic system, loss of physical device or any other similar situation, IT must also be informed.

In instances where there is the potential breach of personal data the DPO must also be informed at the earliest possible point.

The confidentiality or security of information that has been breached which was held in a physical format, i.e. paper record, application form or folder, does not need to be reported to IT in most circumstances, however the Information Security Lead must still be informed.

24.9 Protection from Malicious Software - Futura Learning Partnership and its IT providers shall use software protection to detect and deny intrusion, email filtering and if possible, adopt measures such as SPF, DKIM and DMARC (to stop the organisation's email addresses getting spoofed). Users should not be able to install software on the Organisation's network without prior approval or introduce malicious software via other routes, i.e. the use of unmanaged USB devices.

The Head of IT should have a documented process for Cyber Security, seek formal accreditation of IT processes, or adopt standards that equate to accreditation.

24.10 Removable Media - Any removable media should be supplied and managed by the Organisation and controlled effectively by the use of an asset register. The Register should contain who has which device, when it was issued and who issued it. Frequent auditing of issued devices should take place in order to identify any unknown losses. USB port access should, if possible, be restricted either fully or to a select computer, user, or manged device.

Any external information device that someone wishes to use should be submitted to their manager and IT for approval prior to use. Where PD or information of a sensitive nature may be stored, encryption must be applied to removable media devices.

Encryption should be used as standard on removable devices, this may be in the form of a partitioned and password protected section of a USB Drive or a full device encryption on a standalone device.

24.11 Monitoring System Access and Use - Systems should, where possible, be adopted that can provide an auditable trail of access, this is considerably more important as the type and sensitivity or the information being accessed increases. In terms of physical records, this may be limitation to a single or small number of individuals or a signing in and out form, this may be particularly applicable to records that contain special categories of personal data.

Electronic systems will, in many cases, have event record logs, however Futura Learning Partnership must ensure that they understand how this function works and how it may be used when required, or, if it is inadequate, be able to work with their Head of IT or IT provider to apply any additional software as necessary.

The organisation must make it clear to employees that information contained on the Organisation's system is subject to access and monitoring and that, except in exceptional or agreed circumstances, should not be used for personal reasons by employees. The limitations of this may be defined in the Acceptable Use Policy, contract terms or specific guidelines created for this purpose.

24.12 Accreditation and Assessment of Systems - The Information Security Lead must be assured that new systems, be they physical or electronic, are adequately assessed by the relevant manager, head of IT or responsible person.

Such assessment may not need to be formally documented but demonstration of the assessment must be recorded appropriately. Recognised accreditation will provide a significant level of assurance; however, it must be taken into account with the intended way of using any application.

24.13 System Control Change - Any change made to any system must be confirmed with the Information Owners and, where any conflict arises, must be referred to the Information Security Lead. Access abilities to alter any system parameters should adhere to the Principle of Least Privilege.

24.14 Business Continuity and Disaster Recovery Plans - The Information Security Lead is responsible for ensuring that, in the event of any catastrophic failure of a system, there is adequate capability for the continuation of the use of information in line with the CIA Triad. Any system which is deemed to be critical to the organisation should be included within a Business

Continuity Plan, this may include the Pupil Management System, access to financial resources or safeguarding information.

Cyber Incident Response Plans (CIRP) should be adopted and testing. A CIRP may form part of a disaster recovery plan but should be separately identifiable within that plan.

24.15 Training and Awareness - Information security may not be considered a separate training topic in its own right; however, the CIA Triad should underpin any training in relation to the processing of data. This will include system use and operation, data protection training, safeguarding, and procurement training.

25. Document Classification

The adoption of a document classification system may be used to determine the appropriate level of security that should be applied to data that is held by the organisation. It may not be a possibility to mark individual documents with a protective marker, however, an understanding of the sensitivity of the information, particularly in relation to those identified in section 5, must determine the handling of data.

A determination of what data constitutes a higher risk may be derived from tools such as the Record of Processing Activities (RoPA), Information Asset Registers or localised guidance. Where a system is not partitioned or does not have controls to allow any alteration of security measures, it must be considered to be at the level required by the most sensitive information held.

An example of this may occur where a financial system is used to manage queries as well as hold account specific data, in the case the queries would be require a relatively low level of security whereas the account specific data will require considerably more security.

As shown the data held in a system may not need to be marked, or may not be able to be marked, however when moving data outside of that boundary it should be adequately controlled, i.e. a print out of on-going safeguarding incidents has been removed from the security of its system, in this case it may be necessary to mark the records as confidential and include the name of the owner to whom they may be returned if misplaced.

Levels of classification may be developed to meet your organisations specific requirements:

Protective Marker	Caveat	Covers
Unmarked	None	General information, school updates, public information, newsletters etc.
Confidential	Safeguarding, HR/Personnel,	Generally, information that relates to a person or may be considered personal data which was provided in confidence or may have been discussed without the intention of disclosing it to an individual or individuals.
Sensitive	Finance, HR, Planning, Policy, Contracts	This will cover information that may cause disruption to school business if inadvertently disclosed.

The key principles of data classification and handling are.

- All information, which is created, acquired, or used in support of business activities, must only be used for its intended business purpose.
- All information assets must have an information owner established within the lines of business; this should be defined in the RoPA.
- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information should be classified on an ongoing basis based on its confidentiality, integrity, and availability characteristics.
- An information asset must be classified based on the highest level necessitated by its individual data elements.
- If the Futura Learning Partnership is unable to determine the confidentiality classification of information or the information is personal data, the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- The Futura Learning Partnership must communicate the requirements for secure handling of information to its workforce.

- A written or electronic inventory of all information assets must be maintained. The RoPA will meet this requirement for personal data, however business sensitive information may necessitate an additional register.
- Content made available to the general public must be reviewed according to a process that will be defined and approved by Futura Learning Partnership. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- Personal data must not be made available without appropriate safeguards approved by Futura Learning Partnership.
- For non-public information to be released outside Futura Learning Partnership or shared between other entities, a process must be established that, at a minimum:
    1. Evaluates and documents the sensitivity of the information to be released or shared.
    2. Identifies the responsibilities of each party for protecting the information.
    3. Defines the minimum controls required to transmit and use the information.
    4. Records the measures that each party has in place to protect the information.
    5. Defines a method for compliance measurement.
    6. Provides a signoff procedure for each party to accept responsibilities; and establishes a schedule and procedure for reviewing the controls.

26. Associated Policy and Guidance

- Data Protection Policy
- Data Breach Policy
- Records Management Policy
- Acceptable Use Policy (held within the Online Safety Policy)

Data Protection Impact Assessments

27. Definitions

Initiative - any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity.

Privacy – in its broadest sense the right of an individual to be let alone. It can take two main forms and these can be subject to different types of intrusion:

- **Physical privacy** – the ability of a person to maintain their own physical space or solitude. For example intrusion can come in the form of unwelcome searches of a person's home or acts of surveillance and the taking of biometric information.
- **Information privacy** – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. For example intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of information.

Data Protection Impact Assessment (DPIA) – a process which assists the school in identifying, minimising and addressing the privacy risks associated with any new initiative.

Advice sought and consultation – activity to allow people to highlight privacy risks and solutions based on their own areas of expertise. This can include seeking advice from internal stakeholders or formal consultation with external stakeholders including partners or service users

Information Asset – is current information held by the organisation which is categorised from the perspective of its content/ business use rather than necessarily an IT system. It could be a collection of paper or electronic records held by the school that contain customer/ service user, stakeholder, staff or pupil data. The data the asset holds must be personal and/ or sensitive

Personal data - is information about a person which would enable that person's identity to be established. Sensitive data is anything which if lost or compromised could affect individuals, organisations or the wider community. Sensitive data is defined by the General Data Protection Regulation as including:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- health data

- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning a natural person's sex life or sexual orientation.

28. Background information

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the General Data Protection Regulation.

With so much information being collected, used and shared in the school, it is important that steps are taken to protect the privacy of each individual and ensure that personal information is handled legally, securely, efficiently and effectively.

Completion of a DPIA will assist us to identify and minimise our privacy risks to comply with our data protection obligations and meet individuals' expectations of privacy.

29. The scope of the policy

The policy covers any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity. For the purposes of this policy 'initiative' will cover all of the activity listed above.

The policy provides a process which will enable:

- identification of the need to complete a DPIA through a set of screening questions
- the collection of sufficient information about an initiative to complete a DPIA
- privacy risks identified by the DPIA to be documented and considered.

The process should be followed from the start of an initiative to ensure that potential problems are identified at an early stage, when addressing them will be simpler and less costly and the direction of work can be influenced.

Although the policy is aimed at new initiatives information asset owners may wish to use it as a tool to review existing arrangements to identify and address privacy risks as a continuous improvement activity. Futura Learning Partnership (the trust) policy is that a DPIA shall be carried out for all new and amended initiatives but is not a requirement for existing arrangements.

30. Duties and responsibilities

The Trust Board has overall responsibility for the strategic direction and governance of the trust, including ensuring that school processes comply with all legal, statutory and good practice guidance requirements.

The Chief Operating Officer is responsible to the Board, through the Audit & Risk Committee, for providing information and assurance regarding the management of information risk. Information risk needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

General staff responsibilities – all school staff must follow the requirements of this and related policies particularly those relating to information governance. Particular care should be taken of the privacy impact of working with contractors and partner organisations.

31. The benefits of a DPIA

The completion of a DPIA is a requirement under GDPR and, as such, the ICO may ask an organisation to view a DPIA. It is an effective way to demonstrate to the ICO how personal data processing complies with the GDPR.

The trust can increase pupil, parent and employee confidence in the way it uses and protects their information. An initiative which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A DPIA will demonstrate transparency and may make it easier to explain to individuals why their information is being used.

It will support the trust's legal obligations under the GDPR.

Completing a DPIA in the early stages of an initiative will ensure privacy issues are identified early on and most importantly inappropriate solutions are not implemented that later have to be reversed.

Carrying out a DPIA should benefit the trust through better policies and systems being produced and improving relationships with individuals.

32. The DPIA process – key points

The DPIA process is flexible and can be integrated within the trust's existing approach to managing initiatives including those managed through project management arrangements. Appendix C details an overview of the process. The time and resources dedicated to a DPIA should be scaled to fit the nature of the initiative.

A DPIA should begin early in the life of an initiative and should continue to be considered through to implementation.

The DPIA incorporates the following steps:

- identify the need for a DPIA
- describe the information flows

- identify the privacy and related risks
- identify and evaluate the privacy solutions
- sign off and record the DPIA outcomes
- integrate the outcomes into the key documentation
- consult with internal and external stakeholders as needed throughout the process.

33. Guidance for completion of a DPIA

When should a DPIA be completed?

A DPIA should be completed at the start of any initiative and used to maintain awareness of privacy risks through to completion of work. For procurement activity the DPIA should be completed prior to tender to ensure all relevant privacy risks are considered when preparing specifications.

Who should identify the need for a DPIA and complete it?

It is the responsibility of the lead of an initiative to identify the need for a DPIA and complete it. This may be a process owner, manager of the service area completing the initiative or in the case of formal projects the service lead. The DPIA for a trust-wide initiative will be completed by the trust lead in the area concerned, or a person delegated by the lead.

As a point of principle, it is the responsibility of the lead of an initiative to ensure a DPIA is completed and the DPIA should be completed by someone with an in depth knowledge of the initiative. For example, for an initiative to be introduced in all trust secondary schools, it is likely that the Director of Education will be responsible for ensuring that the DPIA is completed but completion of the DPIA may be delegated to a Principal or other person close to the initiative.

How is the need for a DPIA identified?

The consideration of a number of screening questions will identify the need to complete a DPIA. If any screening question is answered 'yes' a DPIA will need to be completed. The screening questions are detailed in a template attached at appendix D.

How is a DPIA completed?

The template attached at appendix D will guide staff through the completion of a DPIA.

Why is it necessary to describe the information flow in a DPIA?

Understanding the information flows involved in an initiative is essential to a proper assessment of privacy risks. Existing processes and resources such as information audits and the information asset register can be a useful tool in completing this step of a DPIA.

The DPIA template (step two) highlights important information to consider in describing an information flow.

How is a privacy issue identified and a solution evaluated?

When conducting a DPIA it is necessary to identify any privacy risks and their potential consequences for individuals and the trust. The DPIA template (step three) provides a table to record the privacy risks and their consequences. Appendix A provides information about potential privacy risks. The following may also provide useful information:

The ICO's Anonymisation: managing data protection risk code of practice may help to identify privacy risks associated with the use of anonymised personal data.

The ICO's Data sharing code of practice may help to identify privacy risks associated with sharing personal data with other organisations.

The ICO's codes of practice on privacy notices and CCTV, as well as other more specific guidance, will also help to focus DPIAs on those issues.

The DPIA template (step four) provides a table to score the level of risk for each privacy risk identified and to evaluate the solution/s identified by measuring the inherent risk score. Any privacy risk with a residual score of 6 or more should be regarded as high risk by the trust. Such risks may be recorded by the Chief Operating Officer on the corporate risk register.

Why is it necessary to sign off and record the DPIA outcomes?

A key part of the DPIA process is deciding which privacy risks to take forward and recording whether the risks that have been identified are to be tolerated, treated, eliminated or transferred. It may be decided that an identified risk is tolerated. However, if there are unacceptable privacy risks which cannot be treated, eliminated or transferred then it will be necessary to reassess the viability of the initiative or a proposal of that initiative. It is trust policy that the Chief Operating Officer will sign off on all DPIAs.

Who should be consulted?

Consultation and seeking advice is an important part of the DPIA process (and can happen at any stage) allowing people to highlight privacy risks and solutions based on their own areas of expertise.

What documents should be updated?

The DPIA process should be integrated into existing process documents used to plan work required for the initiative. In the case of formal projects this includes the project initiation document (PiD), plan, action/decision, risk/issue log, comms/consultation plan and the equality impact assessment (if appropriate). Decision reports should include reference to the privacy risks and mitigation identified.

Reporting an identified risk?

A key principle of DPIA is that the process is a form of risk management. When carrying out a DPIA, privacy risks to individuals, compliance risks and any related risks for the trust; such as fines for non-compliance with legislation or reputational damage leading to loss of business, should be identified. (Appendix A refers to possible risks to consider)

The template in Appendix D includes a risk assessment approach which should be followed.

Does a DPIA need to be completed for every initiative?

The screening questions must be completed for every initiative. However a DPIA will only be required for initiatives that include personal information and for which a screening question has been answered as yes.

34. Appendices

Appendix 3 – Potential privacy risks

Appendix 4 – Useful links

Appendix 5– Overview of the DPIA process

Appendix 6 – DPIA template – screening questions and assessment

Appendix 3 – Potential privacy risks

The Information Commissioner's Office (ICO) 'Conducting privacy impact assessments code of practice 20140225' version 1.0 details possible privacy risks. This appendix details the relevant extract from the code of practice.

Risks to individuals can be categorised in different ways and it is important that all types of risk are considered – these range from risks to physical safety of individuals, material impacts (such as financial loss) or moral (for example, distress caused). Possible risks include:

Risks to individuals

Inadequate disclosure controls increase the likelihood of information being shared inappropriately. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.

- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with the GDPR or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.

- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the school.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of confidence.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the GDPR
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
- Non-compliance with school specific legislation or standards
- Non-compliance with human rights legislation.

Appendix 4 – Useful links

Information Commissioner's Office - Conducting privacy impact assessments code of practice 20140225 version 1.0

Information Commissioner's Office - Anonymisation: managing data protection risk code of practice

Information Commissioner's Office - Data sharing code of practice

Data Protection Officer- One West

Appendix 5 – Overview of the DPIA process

Step 1: Identifying the need for a DPIA

The need for a DPIA can be identified using the screening questions included in the DPIA template – see Appendix D.

Step 2: Describing the information flows

Describe the information flows of the initiative. Explain what information is collected, used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information. For existing data establish that original consent and privacy notices cover the work being planned/undertaken.

Step 3: Identifying the privacy and related risks

- some will be risks to individuals – for example damage caused by inaccurate data or security breach, or upset caused by unnecessary intrusion on privacy.
- some risks will be to the organisation – for example damage to reputation, or the financial costs of a data breach.
- legal compliance risks include the GDPR, PECR, and the Human Rights Act.

Step 4: Identifying and evaluating privacy solutions

Explain how each risk could be addressed. Some might be eliminated altogether. Other risks might be reduced. Most initiatives will require acceptance of some level of risk and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Consider the available resources, and the need to deliver a project which is still effective.

Step 5: Signing off and recording the DPIA outcomes

All DPIAS will be signed off by the Director of Business and Operations and published on the trust's SharePoint.

Step 6: Integrating the DPIA outcomes back into key documentation

The DPIA findings and actions should be integrated back into key documentation – the DPIA template in Appendix D provides a list of documentation to consider. It might be necessary to return to the DPIA at various stages of the initiative's development and implementation. Large initiatives are more likely to benefit from a formal review process.

A DPIA might generate actions which will continue after the assessment has been finished and these must continue to be monitored.

Appendix 6 – DPIA template

Project information			
Project name		Document version no.	
Author(s)		Version date	
Information asset owner		Project manager (if different)	

Version no.	Version date	Summary of key changes

Do I need to complete a DPIA?	Y/N
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about them?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	

Will the project require you to contact individuals in ways which they may find intrusive?

If you have answered “Yes” to any of the above questions, a DPIA needs to be completed.

1. Outline of the project, objectives and benefits

What does the project aim to achieve, including what the benefits will be to the organisation, to individuals and to other parties?

If this is not a new process, but a change to an existing, please describe the proposed changes.

2. Describe the intended use of personal data

a) Describe the nature of the processing

The nature of the processing is what you plan to do with the personal data. This should include:

- How you collect the data
- How you store the data
- How you use the data
- Who has access to the data
- Who you will and/or may share the data with
- Whether you use any data processors
- Retention period(s)
- Security measures
- Whether there will be any profiling (fully automated decision-making)
- Whether you are using any new technologies
- Whether you are using any novel types of processing

b) Describe the scope of the processing

The scope of the processing is what the processing covers. This should include:

- The nature of the personal data
- The volume and variety of the personal data
- The sensitivity of the personal data
- The extent and frequency of the processing
- The duration of the processing
- The estimated number of the data subjects involved
- The geographical area covered

c) Describe the context of the processing

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- The source of the data
- The nature of your relationship with the individuals
- The extent to which individuals have control over their data
- The extent to which individuals are likely to expect the processing
- Whether they include children or other vulnerable people
- Any previous experience of this type of processing
- Any relevant advances in technology or security
- Any current issues of public concern
- Whether you have considered and complied with any relevant Codes of Practice

d) Describe the purposes of the processing

The purpose of the processing is the reason why you want to process the personal data. This should include:

- Statutory requirement
- Your legitimate interests, where relevant
- The intended outcome for individuals
- The expected benefits for you or for society as a whole
- The impact on the organisation if we don't do it

3. Data protection compliance

Principle 1: Use of personal data is fair, lawful and transparent

This section makes reference to Articles 6, 9 and 10 of GDPR, to demonstrate the lawful basis for carrying out the activity. If in any doubt, please consult your DPO i-west@bathnes.gov.uk

(a) We are relying on the following Article 6 basis for the processing of personal data: (delete lines that don't apply)

Consent
If you are relying on consent, how will the consent be recorded? How can the individuals withdraw their consent?
Necessary for the performance or the setting up of a contract
Necessary for compliance with a legal obligation
State the specific set(s) of legislation
Necessary to protect the vital interests of a person
Necessary for the performance of a task carried out in the public interest, or in the exercise of our official authority
To rely on this condition, the task or function must have a clear basis is law. State the specific set(s) of legislation
Necessary for the pursuit of our legitimate interests
State your legitimate interests State what would happen if this processing didn't happen

(b) We are relying on the following Article 9 basis for the processing special category data: (delete lines that don't apply)

NO SPECIAL CATEGORY DATA
Explicit consent
If you are relying on consent, how will the consent be recorded? How can the individuals withdraw their consent?
Necessary for compliance with employment, social security or social protection law
State which condition of Schedule 1, Part 1 of the Data Protection Act 2018 is met

Necessary to protect the vital interests of a person, where they are physically or legally incapable of giving consent
Processing is carried out by a not-for-profit organisations, and only relates to members of that organisation
The information has been made public by the individual(s)
Necessary for the establishment, exercise or defence of legal claims
Necessary for reasons of substantial interest
State which condition of Schedule 1, Part 2 of the Data Protection Act 2018 is met
Necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
State which condition of Schedule 1, Part 1 of the Data Protection Act 2018 is met
Necessary for reasons of public health
State which condition of Schedule 1, Part 1 of the Data Protection Act 2018 is met
Necessary for archiving, scientific, historical or statistical research
State which condition of Schedule 1, Part 1 of the Data Protection Act 2018 is met

(c) We are relying on the following Article 10 basis for the processing of information relating to criminal convictions or offences: (delete lines that don't apply)

NO INFORMATION RELATING TO CRIMINAL CONVICTIONS OR OFFENCES
We have official authority or statutory functions for law enforcement purposes
State what gives you official authority
The activity meets the following condition(s) within Schedule 1, Parts 1, 2 or 3 of the Data Protection Act 2018
State which condition of Schedule 1 is met

(d) Explain how individuals will be made aware of the processing

(e) If your service is subject to the Human Rights Act:

- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a necessary and proportionate response to the social need?

Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes

(a) If collecting personal data for primary use, explain how you have targeted only the information required

(b) If you are reusing personal data for further use, explain how this secondary use is compatible with the original reason it was collected.

Principle 3: Use of personal data is adequate, relevant and no more than necessary

Explain how the amount of personal data you intend to use is enough to be understood by the audience but no more than the minimum needed to achieve your purpose

Principle 4: Personal data must be accurate and kept up to date

(a) Explain how accurate recording of data will be achieved and how it will be kept up to date, where necessary

(b) Explain any mechanisms that will allow you to amend or append data that is found to be inaccurate

Principle 5: Personal data must be kept in an identifiable format for no longer than is necessary

(a) **Data held in the new IT System:** explain how any automated and / or manual capability to delete data will be used to comply with the corporate retention schedule

(b) **Data held in an unstructured manner (paper, word / excel files etc):** explain how you will use any automated and / or manual capability to delete data in line with the corporate retention schedule

(c) Explain how automatic destruction of individual records can be frozen on request

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction

(a) Explain any technical security measures that will be put in place to protect the data

(b) Explain how you will make staff aware of any security measures or procedures they will need to follow

Articles 15 – 22: Rights of the data subject

Explain how individual rights (requests for subject access, restriction, rectification, objection, erasure and/or portability) will be managed

Articles 44- 49: Transfers of personal data to third countries or international organisations

(a) Explain where the personal data will be hosted, including the routes of transfer if they leave the UK (for example, while most Microsoft cloud services are based in Europe, the data sometimes goes via America)

(b) If the personal data leaves the UK, explain which of the formal / recognised adequacy measures are in place

Demonstration of compliancy with data protection legislation (accountability)

(a) Explain what (if any) governance documents will be required to support the data processing (eg Information Sharing Agreements, Data Processor contractual clauses etc)

(b) Detail what governance arrangements will be in place to oversee the processing of personal data in a compliant manner

4. Consultation
(a) The following consultation approach and stakeholder groups were incorporated into the consultation process:
(b) A summary of the stakeholder views:
(c) The following stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities:
(d) The following stakeholder views were considered, but not reflected in the planned data processing activities:
(e) The rationale for not doing so:

Data Protection Impact Assessment

Risk assessment

Privacy issue	*Identify the key privacy risks and associated compliance and corporate risks*			*Describe the actions you could take to reduce the risks*		
	Risk to individual	**Compliance risk**	**Corporate risk**	**Solution(s)**	**Result** *High, medium or low*	**Evaluation** *Is the solution a justified, compliant and proportionate response?*

Data Protection Impact Assessment

Outcomes

Risk	Approved solution and actions	Approved by	Completion due date	Who is responsible?

DPIA authorisation	
Date of consultation with DPO	
Summary of DPO advice	
DPO advice accepted or over-ruled by IAO	
Rationale for over-ruling the DPO's advice (if applicable)	
Date and name of person referring DPIA to ICO (if applicable)	
Summary of ICO advice	
Date and name of person updating Record of Processing Activity	

Data Breach Policy

35. Introduction

Futura Learning Partnership issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

36. Scope

This policy applies to all employees of Futura Learning Partnership including contract, agency and temporary staff, volunteers and employees of partner organisations working for Futura Learning Partnership.

37. Data Breaches

For the purposes of this policy data breaches will include both 'near misses' and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data)
- Unauthorised use of, access to, or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Hacking attack
- Unforeseen circumstances (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked

- Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

38. Risk Assessment and Reporting

The quick response to a suspected or actual data breach is key. When a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, appropriate steps should be promptly taken to address it.

The focus of risk regarding breach reporting is on the potential negative consequences for individuals. On becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

All parties in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours, this should be reported as soon as practically possible to the person responsible for the management of personal data breaches within the organisation. This should be done through the completion of the reporting form in Appendix 3, which should be sent to your Data Protection Lead, who will liaise with its Data Protection Officer (One West).

Notify the ICO (if necessary) - If the personal data breach is likely to result in a risk to the rights and freedoms of an individual(s), the incident may need to be reported to the Information Commissioner's Office (ICO), no later than 72 hours after becoming aware of the breach. It is, therefore, crucial that you report any data breach (regardless of the severity) to your Data Protection Officer (DPO) as soon practically possible. It is especially important to report data breaches as promptly where there is low staff availability and or a Bank Holiday. The DPO will advise on whether to notify the ICO, however the final decision will rest with the organisation. If a decision to report is made, then it is the organisation's responsibility to liaise with the ICO to ensure the report is sent off. If you need to report an incident to the ICO please liaise with Director of Business and Operations before making the notification.

Notify data subjects (if necessary) - If the breach is likely to result in a high risk to the rights and freedoms of individuals then you should promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach. When notifying individuals, you should consider including the following:

- Outline what has occurred and apologise.
- Provide name and contact details of lead officer or relevant manager for further information.
- Describe any likely consequences.
- Describe any measures taken or proposed to be taken to address the breach including any measures to mitigate its possible adverse effects.
- Advise whether the ICO has been notified.

- Record notification to the data subject in breach log.

39. Monitoring and Compliance

Compliance with this policy shall be monitored through a review process managed by the Director of Business and Operations. All personal data breaches (and near misses) should be recorded whether or not they have been reported to the ICO. The breach log will include the facts of the breach, its effects and the remedial action taken. Staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken.

Learning from experience

The relevant manager should, in consultation with the DPO, undertake a review of existing controls to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review should consider:

- Whether policy controls are sufficient
- Whether the breach occurred due to system error or human error or both
- Whether training and awareness can be amended and/or improved (if a report to the ICO is made, they are likely to seek details of training that has been undertaken)
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- If *learning from experience* to be disseminated to all staff (where possible without identifying the person responsible).

40. Links with Other Policies

This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Staff Acceptable Usage Policy in Online Safety Policy
- Online Safety
- IT Security Policy

Appendix 7 – Data Breach Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation *If there was any delay in reporting the incident, please explain why this was*	
Who notified the organisation of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why? *Identifying information should be anonymised for any reporting purposes.*	
2. Recovery of the data	
What have you done to contain the incident? *eg limiting the initial damage, isolating affected systems, notifying the police where necessary, providing support to affected data subjects*	
Please provide details of how you have recovered or attempted to recover the data, and when *Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*	
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	

Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals indicated that they may or have already made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your Organisation: **Your name and contact details:**	

Records Management Policy

41. Introduction

Futura Learning Partnership recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and contribute to the effective overall management of the organisation. Records provide evidence for protecting the legal rights and interests of the organisation and provide evidence for demonstrating performance and accountability. The aim of this policy is to provide a framework for managing the organisation's information to enable the organisation to:

- Make informed decisions;
- Be open and transparent;
- Respond appropriately to information requests;
- Protect records;
- Comply with the legislative requirements;
- Effectively work with its partners, and share information as required;
- Demonstrate accountability.

42. Objectives

The objective of this policy is to define a framework for Futura Learning Partnership to manage data, information, and records.

43. Definitions

Data – Raw facts and figures that supply the basis for information.

Information – Data which has been collected, organised, ordered and given both meaning and context.

Record – Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations, or in the transaction of business.

Confidential Waste – See Appendix 4.

44. Scope

This policy applies to all employees of Futura Learning Partnership including contract, agency and temporary staff, volunteers and employees of partner organisations working on behalf of Futura Learning Partnership.

All records created, held, and maintained by Futura Learning Partnership in the course of its duties are covered by this policy. This is irrespective of the format of the information, including, but not limited to:

- Paper records
- Electronic records (Word Documents, emails, PowerPoints, database, etc.)

- Photographs, videos, etc.
- Electronic storage media (floppy disc, CDs, DVD and memory sticks)

45. Responsibilities

The organisation has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Director of Business & Operations.

The person responsible for records management in the organisation will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way.

All members of staff and employees are individually responsible for the records they create or hold. Individuals must ensure that records are accurate, maintained securely, and disposed of in accordance with this policy.

46. Creation & Storage

All organisation staff are responsible for creating and maintaining data, information and records in relation to their work, and storing them in a way which ensures that they can be identified and retrieved when required.

Records must be appropriately stored with due regard for efficiency, cost-effectiveness, security, durability, and access. Appropriate procedures and processes are in place to ensure the physical and intellectual security of organisation records. Please refer to Data Protection Policy and/or Information Security Policy for more details.

Storage conditions and handling processes should be designed to protect records from unauthorised access, loss, destruction, theft, and disaster. This in line with the UK General Data Protection Regulation (UK GDPR) principles of data protection by design, and integrity and confidentiality.

The retention of records for longer than necessary is in breach of the UK GDPR, and the duplication of records should be limited to optimise the use of space for storage purposes and to aid data accuracy.

47. Retention and Disposal

Information held for longer than is necessary carries additional risk and cost, therefore records and information shall only be retained when there is a business or legislative need to do so. Under the UK GDPR and the Data Protection Act 2018 (DPA 2018), personal data processed by an organisation must not be retained for longer than is necessary for its lawful purpose.

The retention of specific documents may be necessary to:

- Fulfil statutory or other regulatory requirements.[1]
- Evidence events/agreements in the case of disputes.

[1] The Covid-19 Public Inquiry issued a Document Preservation Notice on 11th November 2022. This inquiry will cover all aspects of the country's response to the Covid-19 pandemic and requires organisations to preserve all documents relating to the pandemic and the following recovery period. For more information about the inquiry visit: https://covid19.public-inquiry.uk/.

- Meet operational needs.
- Ensure the preservation of documents of historic or other value.
- Evidence child protection matters.

The untimely destruction of documents could cause the organisation :

- Difficulty in defending litigious claims
- Operational problems
- Embarrassment
- Failure to comply with the Freedom of Information or Data Protection laws.

Conversely, the permanent retention of all documents where there is no business need or other legal basis to retain them, poses regulatory and security risks, as well as being a breach of personal data.

Appropriate secure disposal is accordingly implemented at the organisation in accordance with the organisation's retention schedule for the following reasons:

- To comply with Article 5 of the UK GDPR which states that personal data must not be kept in an identifiable form for longer than is necessary
- To free-up storage space (there is evidence that the de-cluttering of office accommodation can be psychologically beneficial for employees.);
- To reduce the risk of fire (in the case of paper records);
- To lessen the risk of a data breach through data loss or unauthorised access.
- To increase the efficiency of the exercising of data subject rights.

47.1 Retention Schedule

In line with all relevant legislative requirements, including the UK GDPR and DPA 2018, Futura Learning Partnership will keep some forms of information for longer than others. Information will not be kept indefinitely unless there are specific requirements.

The organisation maintains records in line with its Retention Schedule - See Appendix 5.

47.2 Definition of Retention Periods

Defining a retention period will be determined on one of the following three factors:

- Statutory requirements.
- Codes of Practice and guidance published by professional bodies.
- In the absence of the above, the retention period will be determined by the needs of the trust.

Defining the retention period based on organisation needs must be approved by the ELG or relevant senior manager and where necessary in consultation with the DPO.

47.3 Reviewing Retention Periods

Most retention periods will remain static and will relate to legal requirements to retain data. However, retention periods based on codes of practice and guidance published by professional bodies may vary. Any changes to known retention periods should be raised with the Director of Business and Operations and where necessary the DPO.

This Policy and retention schedule should be reviewed annually or where any other cause requires its immediate correction.

47.4 Course of Action at the End of the Retention Period

When a record reaches the end of its retention period in most cases it will be deleted or destroyed. However, these are not the only courses of action that can be taken, and consideration must be made to the relevance of the data for other uses.

In most cases the requirement for further use of data will be identified prior to processing, however there may be occasion where a dataset is identified as having particular relevance to the needs of the organisation .

The following may occur to data after the period of use has expired:

- Anonymisation for statistical needs.
- Transfer to an appropriate archive where it is in the public interest.
- Scientific or historical research purposes.

Appropriate safeguards must be put in place to ensure that wherever personal data is used beyond its original period of retention it is done so legally and in compliance with DPA 2018 and guidance from the Information Commissioner's Office (ICO).

47.5 Disposal

The organisation will use an accredited confidential waste disposal provider / shred the information on site using a cross-cut shredder. Information on what should be deemed as confidential waste is detailed in Appendix 4.

Wherever practicable and appropriately secure, disposal methods should encourage recycling.

Electronic files are securely overwritten, in accordance with government guidance, and other media is shredded, incinerated, or otherwise disintegrated for data in line with IT policies.

The disposal of the organisation's data, in either paper or electronic form, is conducted in a way that makes reconstruction highly unlikely. Once data has been deleted, it is deemed to be a permanent deletion, irrespective of whether it could technically be reconstructed from a back-up.

Under no circumstances should paper documents containing personal data or confidential information be simply binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties and render the organisation liable to enforcement action by the Information Commissioner's Office.

If records are accidentally destroyed or discovered, this should be reported as a data breach to DP Lead, in line with the Data Breach Policy.

47.6 Archiving

A small percentage of the school's records may be selected for permanent preservation as part of the trust's archives. It is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations of former pupils; and to serve as a research resource for all interested in the history of Futura Learning Partnership and the community it serves.

47.7 Protective Marking

Protective markings may be written upon documentation where it is used in physical forms. In general, the classification of documentation will relate more specifically to the handling and access that is permitted to that data. Confidential data related to employment purposes for example should only be accessible by HR staff or direct line managers for specific reasons.

Information deemed to be financially sensitive, or business sensitive may for the purposes of requests made under the Freedom of Information Act be exempt and, in any case, should be handled with more caution than general data.

48. Monitoring and Compliance

This policy is reviewed annually.

Compliance with this policy shall be monitored through a review process undertaken by the person with overall responsibility for records management within the organisation. This will be achieved by an annual survey to check if records are stored securely and can be accessed appropriately.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, Futura Learning Partnership, in consultation with senior management and our Data Protection Officer, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

49. Relationship with Existing Policies

This policy has been drawn up within the context of:

- Data Protection Policy
- Data Breach Policy
- Information Security Policy
- IT Security Policy

Appendix 8- What is Confidential Waste?

(1) Any record* which details personal information

What is personal information?

- Relates to and identifies a living person
- Could help someone identify a person when used with other information

- Is an expression of opinion about an individual
- Indicates our intentions towards an individual

Such as: Name, Address, Date of Birth, Email, Phone numbers, Location data, IP addresses

(2) Any record* which details special categories of personal data

What are special categories of personal data?

- Racial and/or Ethnic Origin
- Political Opinions
- Religious Beliefs (or other beliefs of a similar nature)
- Trade Union membership
- Biometric Information e.g. Photos
- Mental or Physical Health condition
- Sexual life and Orientation
- Criminal Records are afforded similar protections to special category data and are similarly sensitive

Such as: Safeguarding, Accident/First Aid, Equalities information, Legal records

(3) Any record* which details business/commercially sensitive information

What is business/commercially sensitive information?

- Information which Futura Learning Partnership would be affected by any loss of, or unauthorised access to.

Such as: Contracts, opinions on service delivery, tender information.

If you have any doubt, then please treat the information as Confidential

** A Record can be in many formats – e.g. Paper, Post-it notes, Disks, CDs, Tapes, Posters, Emails, etc*

Appendix 9- Retention Schedule

Governance and School Management

This section covers the work of the Trust Board, Academy Governance Committees (AGC), the Executive Leadership Team, Headteachers/Principals and their senior leadership teams, the admissions process and operational administration.

1.1 AGC

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
1.1.1	Agendas for Board/Committee/AGC meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		PERMANENT	
1.1.2	Minutes of Board/Committee/AGC meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		PERMANENT	

1.1.3	Reports presented to the Board/Committees/AGC	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	.
1.1.6	Trusts and Endowments managed by the Trust Board or an AGC	No		PERMANENT	
1.1.7	Action plans / development plans	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Trust Board or an AGC	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Trust Board or an AGC	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Headteacher / Principal and Senior Leadership Team

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the Headteacher / Principal	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	
1.2.2	Minutes of Senior Leadership Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Headteacher / Principal or the Leadership Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL

1.2.4	Records created by Headteachers / Principals, deputy Head Teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by Headteachers / Principals, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL
1.2.8	Subject Access Requests	Yes		Date of the response to the request +7 years	SECURE DISPOSAL

Admissions Process

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code. Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels, 2021	Life of the policy + 3 years then review	SECURE DISPOSAL

1.3.2	Admissions – if an appeal is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels, 2021	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if an appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels, 2021	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made[1]	REVIEW. Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school
1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels, 2021	Current year + 1 year	SECURE DISPOSAL

School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014 p6

Admissions Process

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc.	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
1.4.1	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.2	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.3	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.5	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

Human Resources

2.1 Recruitment

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new Headteacher/Principal	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education (2022) (Statutory Guidance from Dept. of Education) Sections 275-277	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation	

				then this should be placed on the member of staff's personal file	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[2]	Yes	An employer's guide to right to work checks (Home Office)	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

Employers are required to take a "clear copy" of the documents which they are shown as part of this process

Operational Staff Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

Management of Disciplinary and Grievance Processes

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children, July 2018"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning3+ 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	written warning – level 1			Date of warning + 6 months	
	written warning – level 2			Date of warning + 12 months	
	final warning			Date of warning + 18 months	
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice

2.4 Health and Safety

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL

2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

2.5 Payroll and Pensions

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

Financial management of the trust

This section deals with all aspects of the financial management of the trust including the administration of school meals.

3.1 Risk Management and Insurance					
	Basic file description	**Data Protection Issues**	Statutory Provisions	**Retention Period [Operational]**	**Action within 12 months of the end of the administrative life of the record**
3.1.1	Employer's Liability Insurance Certificate and other insurance certificates	No		Closure of the school + 40 years	SECURE DISPOSAL
3.1.2	Insurance claims – copies of correspondence	Yes			

3.2 Asset Management					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action within 12 months of the end of the administrative life of the record**
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the trust	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement, background papers, management accounts	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL

3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action within 12 months of the end of the administrative life of the record**
4.1.1	Title deeds of properties belonging to the trust	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the trust	No		These should be retained whilst the building belongs to the trust and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the trust	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of trust premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
4.2.1	All records relating to the maintenance of trust premises carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the trust premises carried out by trust employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school The file should follow the pupil when he/she leaves the primary school. This will include to another primary school, to a secondary school, or a pupil referral unit If the pupil dies whilst at primary school or transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period.	
	Secondary	Limitation Act 1980 (Section 2)		Date of Birth of the pupil + 25 years	SECURE DISPOSAL

5.1 Pupil's Educational Record

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter- agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter- agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review. This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule

5.2 Attendance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	Working Together to Improve Attendance (Sep 2022) Education Regulations (Pupil Attendance) 2006	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record

5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

Curriculum Management

6.1 Statistics and Management Information

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action within 12 months of the end of the administrative life of the record**
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

Extra-Curricular Activities

7.1 Educational Visits outside the Classroom

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.

7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2 Walking Bus

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back-up copies should be destroyed at the same time]

7.3 Miscellaneous

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes		While the referral is current	
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6	Group Registers	Yes		Current year + 2 years	

Central Government and Local Authority

This section covers records created in the course of interaction between the trust and the local authority.

8.1 Local Authority

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL

8.2 Central Government

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action within 12 months of the end of the administrative life of the record
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL

8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

Appendix 10 - Quick Calculators

Quick calculator - ACADEMIC YEARS - DISPOSAL BY 31.08.23

Production Date/Retention Period ACADEMIC YEARS	Current year + 1 year	Current year + 2 years	Current year + 3 years	Current year + 5 years	Current year + 6 years
2020/21	DISPOSE*	RETAIN	RETAIN	RETAIN	RETAIN
2019/20	OVERDUE FOR DISPOSAL	DISPOSE*	RETAIN	RETAIN	RETAIN
2018/19	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	DISPOSE*	RETAIN	RETAIN
2017/18	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	RETAIN	RETAIN
2016/17	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	DISPOSE*	RETAIN
2015/16	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	DISPOSE*
Pre Sep 2015	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL

*REVIEW FIRST IN LINE WITH THE RETENTION SCHEDULE

Quick calculator- CALENDAR YEARS - DISPOSAL BY 31.12.23

Production Date/Retention Period CALENDAR YEARS	Current year + 1 year	Current year + 2 years	Current year + 3 years	Current year + 5 years	Current year + 6 years
2021	DISPOSE*	RETAIN	RETAIN	RETAIN	RETAIN
2020	OVERDUE FOR DISPOSAL	DISPOSE*	RETAIN	RETAIN	RETAIN
2019	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	DISPOSE*	RETAIN	RETAIN
2018	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	RETAIN	RETAIN
2017	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	DISPOSE *	RETAIN
2016	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	DISPOSE*
Pre 2016	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL	OVERDUE FOR DISPOSAL

*REVIEW FIRST IN LINE WITH THE RETENTION SCHEDULE

Quick calculator- FIXED PERIOD

FIXED DATE IN…./Retention Period	+1 year	+3 years	+6 years	7 years	+10 years	+12 years	+14 years	+25 years	+40 years	+50 years
2023	2024	2026	2029	2030	2033	2035	2037	2048	2063	2073
2022	2023	2025	2028	2029	2032	2034	2036	2047	2062	2072
2021	2022	2024	2027	2028	2031	2033	2035	2046	2061	2071
2020	2021	2023	2026	2027	2030	2032	2034	2045	2060	2070
2019	2020	2022	2025	2026	2029	2031	2033	2044	2059	2069
2018	2019	2021	2024	2025	2028	2030	2032	2043	2058	2068
2017	2018	2020	2023	2024	2027	2029	2031	2042	2057	2067
2016	2017	2019	2022	2023	2026	2028	2030	2041	2056	2066
2015	2016	2018	2021	2022	2025	2027	2029	2040	2055	2065
2014	2015	2017	2020	2021	2024	2026	2028	2039	2054	2064
2013	2014	2016	2019	2020	2023	2025	2027	2038	2053	2063
2012	2013	2015	2018	2019	2022	2024	2026	2037	2052	2062
2011	2012	2014	2017	2018	2021	2023	2025	2036	2051	2061
2010	2011	2013	2016	2017	2020	2022	2024	2035	2050	2060
2009	2010	2012	2015	2016	2019	2021	2023	2034	2049	2059

FIXED DATE IN…./Retention Period	+1 year	+3 years	+6 years	+7 years	+10 years	+12 years	+14 years	+25 years	+40 years	+50 years
2008	2009	2011	2014	2015	2018	2020	2022	2033	2048	2058
2007	2008	2010	2013	2014	2017	2019	2021	2032	2047	2057
2006	2007	2009	2012	2013	2016	2018	2020	2031	2046	2056
2005	2006	2008	2011	2012	2015	2017	2019	2030	2045	2055
2004	2005	2007	2010	2011	2014	2016	2018	2029	2044	2054
2003	2004	2006	2009	2010	2013	2015	2017	2028	2043	2053
2002	2003	2005	2008	2009	2012	2014	2016	2027	2042	2052
2001	2002	2004	2007	2008	2011	2013	2015	2026	2041	2051
2000	2001	2003	2006	2007	2010	2012	2014	2025	2040	2050
1999	2000	2002	2005	2006	2009	2011	2013	2024	2039	2049
1998	1999	2001	2004	2005	2008	2010	2012	2023	2038	2048
1997	1998	2000	2003	2004	2007	2009	2011	2022	2037	2047
1996	1997	1999	2002	2003	2006	2008	2010	2021	2036	2046
1995	1996	1998	2001	2002	2005	2007	2009	2020	2035	2045
1994	1995	1997	2000	2001	2004	2006	2008	2019	2034	2044
1993	1994	1996	1999	2000	2003	2005	2007	2018	2033	2043

FIXED DATE IN…./Retention Period	+1 year	+3 years	+6 years	+7 years	+10 years	+12 years	+14 years	+25 years	+40 years	+50 years
1992	1993	1995	1998	1999	2002	2004	2006	2017	2032	2042
1991	1992	1994	1997	1998	2001	2003	2005	2016	2031	2041
1990	1991	1993	1996	1997	2000	2002	2004	2015	2030	2040
1989	1990	1992	1995	1996	1999	2001	2003	2014	2029	2039
1988	1989	1991	1994	1995	1998	2000	2002	2013	2028	2038
1987	1988	1990	1993	1994	1997	1999	2001	2012	2027	2037
1986	1987	1989	1992	1993	1996	1998	2000	2011	2026	2036
1985	1986	1988	1991	1992	1995	1997	1999	2010	2025	2035
1984	1985	1987	1990	1991	1994	1996	1998	2009	2024	2034
1983	1984	1986	1989	1990	1993	1995	1997	2008	2023	2033
1982	1983	1985	1988	1989	1992	1994	1996	2007	2022	2033
1981	1982	1984	1987	1988	1991	1993	1995	2006	2021	2032
1980	1981	1983	1986	1987	1990	1992	1994	2005	2020	2031
1979	1980	1982	1985	1986	1989	1991	1993	2004	2019	2030
1978	1979	1981	1984	1985	1988	1990	1992	2003	2018	2029

1977	1978	1980	1983	1984	1987	1989	1991	2002	2017	2028

FIXED DATE IN…./Retention Period	+1 year	+3 years	+6 years	+7 years	+10 years	+12 years	+14 years	+25 years	+40 years	+50 years
1976	1977	1979	1982	1983	1986	1988	1990	2001	2016	2026
1975	1976	1978	1981	1982	1985	1987	1989	2000	2015	2025
1974	1975	1977	1980	1981	1984	1986	1988	1999	2014	2024
1973	1974	1976	1979	1980	1983	1985	1987	1998	2013	2023
Pre 1973	Pre 1974	Pre 1976	Pre 1979	Pre 1980	Pre 1983	Pre 1985	Pre 1987	Pre 1998	Pre 2013	Pre 2023