Data Protection Policy

Contents

Policy statement

1 During the course of our activities as a Trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others.

2 We are committed to the protection of all **personal data a**nd **special category personal data** and this policy sets out how we comply with relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.

3 All **data users** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

About this policy

4 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ("**GDPR**"), the Data Protection Act 2018, and other regulations (together "**data protection legislation"**).

5 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

6 This policy does not form part of any employee's contract of employment and may be amended at any time.

7 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

Definition of data protection terms

All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

Data Protection Officer

8 As a Trust we are required to appoint a Data Protection Officer ("**DPO**"). Our DPO is Linda Vaughan, and they can be contacted at enquiry@excelsiormat.org.

9 The DPO is responsible for informing and advising the Trust about **data protection legislation**, ensuring compliance with the law and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

10 The DPO is also the central point of contact for all data subjects, **the Information Commission** ("**IC**") and others in relation to matters of data protection.

Our data protection commitments

11 We are dedicated to ensuring that **personal data** is processed in alignment with the legal principles of data protection;

12 We implement a strategy focused on "Data Protection by Design and Default";

13 We can prove our adherence to **data protection legislation**;

14 **Data subjects** are well-informed about how and why we use their data, and they can exercise their rights regarding their data;

15 We share **personal data** only when it is fair and lawful, ensuring that any data sharing is conducted securely;

16 We handle and report all **personal data breaches**, including minor ones, effectively to mitigate any potential risks and to improve our practices;

Data protection principles

17 Anyone **processing personal data** must comply with the data protection principles. We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

18 The principles provide that **personal data** must be:

18.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**. This means that we only use **personal data** with respect for the individual who it relates to, in line with the legal grounds for **processing** and we inform **data subjects** how their data is processed including, among other ways, in our **privacy notices**;

18.2 **Processed** for specified, explicit and legitimate purposes and in a way which is not incompatible with those purposes. This means that if we collect data for one purpose and then need to use it for another reason we will ensure that new purpose is compatible with the original reason for **processing**;

18.3 Adequate, relevant and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required;

18.4 Accurate and up to date. This means that we will try to ensure that data is accurate when we collect it, and kept up-to-date over time;

18.5 Not kept for any longer than is necessary for the purpose. This means that we only keep personal data for as long as it is necessary and we comply with our Records Management and Retention Policy; and

18.6 **Processed** securely using appropriate technical and organisational measures. Our measures include: technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms, and encryption; as well as organisational safeguards including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

19 **Personal Data** must also:

19.1 be **processed** in line with **data subjects'** rights;

19.2 not be transferred to people or organisations situated in other countries without adequate protection.

Legal grounds for processing

20 For **personal data** to be **processed** lawfully, it must be **processed** based on one of the legal grounds set out in the **data protection legislation**. We will normally **process personal data** under the following legal grounds:

20.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

20.2 where the **processing** is necessary to comply with a legal obligation that we are subject to;

20.3 where the **processing** is necessary in order to protect the vital interests of a **data subject** or another individual;

20.4 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest;

20.5 where the **processing** is necessary for the purposes of a recognised legitimate interest as set out in Annex 1 of the **GDPR**;

20.6 where the **processing** is necessary for the purposes of our legitimate interests (or the legitimate interests of a third party) except where such interests are overridden by the interests and fundamental rights and freedoms of the **data subject**; and

20.7 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

21 When **special category personal data is** being processed then an additional legal ground must apply to that **processing**. We will normally only process **special category personal data** under following legal grounds:

21.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

22 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

22.1 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

22.2 where none of the above apply then we will seek the explicit consent of the **data subject** to the **processing** of their **special category personal data**.

23 We will inform **data subjects** of the above matters by way of appropriate **privacy notices** which shall be provided to them when we collect the data or as soon as possible thereafter unless we have already provided this information such as at the time when a pupil joins us.

24 If any **data user** is in doubt as to the legal ground for processing, then they must contact the DPO before doing so.

Vital Interests

25 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not able to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

26 Where none of the other bases for **processing** set out above apply then the Trust must seek the consent of the **data subject** before **processing** any personal data for any purpose.

27 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

28 When pupils and or our **workforce** join the Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

29 In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

30 We will generally seek consent directly from a pupil who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

31 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

31.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

31.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

31.3 Inform the **data subject** of how they can withdraw their consent.

32 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent. We will ensure that it will be as easy for the **data subject** to withdraw their consent as it was to give it.

33 The DPO must always be consulted in relation to any consent form before consent is obtained.

34 A record must always be kept of any consent, including how it was obtained and when.

Data subjects' rights

35 In addition to the right to be informed and the right to withdraw consent, we will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

35.1 request access to any **personal data** we hold about them;

35.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

35.3 have inaccurate or incomplete **personal data** about them rectified;

35.4 restrict processing of their **personal data**;

35.5 have **personal data** we hold about them erased; and

35.6 object to the making of decisions about them by automated means.

36 The rights available to **data subjects** will depend on the lawful basis for **processing**, for example, where **personal data** is **processed** under the lawful basis of public task, then the **data subject** cannot withdraw consent for such **processing**, but they exercise the right of objection.

37 Except for the right to object to direct marketing, other rights requests in an education or employment context can be complex. We will comply with our obligations under **data protection laws** and the guidance given by the **IC** in respect of individuals seeking to exercise their rights.

38 We will consider **data subject** requests and provide a response within one month, except if we consider the issue to be too complex to resolve within that period then we

may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

39 Where we are unable to grant **data subjects** any requests made as part of their rights, for example, where we are unable to delete data as we are required to retain it in relation to any claim or legal proceedings, we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the **IC** at the time that we inform them of our decision in relation to their request.

40 The DPO must be consulted in relation to any **data subject** rights requests.

The Right of Access to Personal Data

41 **Data subjects** may request access to **personal data** we hold about them. Such requests will be considered in line with the Trust's Subject Access Request Procedure.

Data protection by design and default

42 The Trust will consider and comply with the requirements of **data protection legislation** in relation to all its activities whenever these involve the use of **personal data**, in accordance with the principles of data protection by design and default.

43 In certain circumstances the law requires us to carry out detailed assessments of proposed processing in a **Data Protection Impact Assessment** ("**DPIA**"). This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or there is a change in our existing ways of working.

44 The Trust will complete a **DPIA** for such proposed **processing** and has a template document which ensures that all relevant matters are considered. We may also carry out **DPIAs** where one is not legally required, as a matter of good practice.

45 The DPO should always be consulted as to whether a **DPIA** is required, and if so how to undertake that assessment. The DPO must always be consulted where **personal data** is to be transferred to different countries to ensure adequate protection is in place.

46 We carry out and review **DPIAs** in accordance with our DPIA procedure.

Data security

47 We will take appropriate security measures against unlawful or unauthorised **processing** of **personal data**, and against the accidental loss of, or damage to, **personal data**.

48 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

49 Security procedures include:

49.1 Entry controls. Any stranger seen in entry-controlled areas should be challenged. Any such incident must also be reported to the Headteacher.

49.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (**Personal data** is always considered confidential).

49.3 Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with **IC** guidance on the disposal of IT assets.

49.4 Equipment. **Data users** must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

49.5 Working away from the school premises – paper documents. Paper documents should only be removed from the premises if absolutely necessary and should be transported securely.

49.6 Working away from the school premises – electronic working. All documents must be saved onto the Trust One Drive. USBs are not permitted.

49.7 Document printing. Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

50 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Personal data breaches

51 The Trust recognises that a breach of **personal data** could happen, despite our policies, procedures and measures in place to protect **personal data**, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.

52 The Trust Personal Data Breach Procedure supports this policy and must be followed in relation to any actual or suspected breach of **personal data.**

Disclosure and sharing of personal information

53 We may share **personal data** that we hold about **data subjects** with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so[1].

54 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

[1] Welsh schools should refer to Welsh government bodies including Estyn

55 Where necessary we will enter into data sharing agreements to help facilitate the safe sharing of **personal data**.

56 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Data processors

57 We contract with various organisations who provide services to the Trust. These include people, companies, and systems that process personal data on our behalf and under our instruction.

58 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

59 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

60 Contracts with **data processors** will comply with **data protection legislation** and contain explicit obligations on the **data processor** to ensure compliance with the **data protection legislation**, and compliance with the rights of **data subjects**.

Images and Videos

61 Parents and others attending School events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

62 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

63 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

64 Whenever a pupil begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, or their

parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

Complaints

65 **Data subjects** have the right to make a complaint to the Trust if they consider we have not complied with **data protection legislation**. Any complaints relating to data protection must be directed to our **Data Protection Officer**.

66 When dealing with complaints relating to data protection, we shall:

66.1 Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by the Trust;

66.2 Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate;

66.3 Inform the complainant about progress of the complaint; and

67 Inform the complainant of the outcome of the complaint.

Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Annex: Definitions

Term	Definition
Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	are those of our workforce (including Governors, temporary or agency staff and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Term	Definition
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data Protection Impact Assessment (DPIA)	a tool to help identify how to comply with data protection obligations and protect individuals' rights as set out in Article 35 of the UK GDPR. The IC also has guidance on DPIAs on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
Data Protection Legislation	Means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended by the Data (Use and Access) Act 2025; and all other legislation and regulatory requirements in force from time to time which apply to the use of personal data.
Information Commission (IC)	in the UK, the Information Commission (IC) is the data protection regulator. The website of the IC is at www.ico.org.uk.
Privacy notices	where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as Data Controller and those of the DPO; the purpose or purposes and legal basis for which we intend to process that personal data; the types of third parties, if any, with which we will share or to which we will disclose that personal data; whether the personal data will be transferred outside the UK and if so the safeguards in place; the period for which their personal data will be stored, by reference to our Records Management and Retention Policy; the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the IC.
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording,

Term	Definition
	organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes, any individual employed by Excelsior Multi Academy Trust such as staff and those who volunteer in any capacity including Governors and/or Trustees / Members.