Waveney Valley
Academies Trust

DATA PROTECTION POLICY

12/10/2021

Contents

1. Aims

Waveney Valley Academies Trust is committed to being transparent about how it collects and uses the personal data of its staff, children, parents and carers, and to meeting its data protection obligations.

This policy sets out the Trust's commitment to data protection, and individual rights and obligations in relation to personal data.

2. Legislation and guidance

This policy meets the requirements of General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act (DPA) 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Any action relating to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. Data protection principles

Waveney Valley Academies Trust and all our Academies process personal data in accordance with the following data protection principles:

- Process personal data lawfully, fairly and in a transparent manner.
- Collect personal data only for specified, explicit and legitimate purposes.
- Process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keep accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keep personal data only for the period necessary for processing.
- Adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Waveney Valley Academies Trust and all our Academies tell individuals the reasons for processing their personal data, how such data will be used and the legal basis for processing in our privacy notices.

Where Waveney Valley Academies Trust and our Academies process special categories of personal data, or criminal records, to perform obligations or to exercise rights in employment law, this is done in accordance with the General Data Protection Regulation (GDPR).

Waveney Valley Academies Trust and our Academies will update personal data promptly if an individual advises that their information has changed or is inaccurate and data gathered is held in:

- the individual's personnel file (in hard copy or electronic format, or both)
- on HR systems
- in pupil/student files

The periods for which we hold personal data are contained in our privacy notices/retention schedule and we keep a record of our processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

We process personal data relating to individuals as part of our educational operations and the Trust is, therefore, recognised as a data controller.

The Trust is registered as a data controller with the ICO and this registration will be renewed annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to all employees of Waveney Valley Academies Trust, and to any external organisations or individuals working on the Trust's behalf.

5.1 The Trust Board

The Waveney Valley Academies Trust Board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

Waveney Valley Academies Trust has contracted School's Choice Data Protection service to act as our data protection officer. Their role is to inform and advise the school on its data protection obligations. They can be contacted at Data.Protection@schoolschoice.org and questions about this policy, or requests for further information, should be directed to them.

5.3 Chief Executive Officer (CEO)

The CEO takes responsibility on behalf of the data controller on a day-to-day basis.

5.4 Data Protection Representative (DPR)

The DPR acts as a representative for the data controller on a day-to-day basis, liaising with the DPO.

5.5 Data Protection Contacts

All Academies within the Trust have a nominated Data Protection Contact (DPC). The DPC is the first point of contact for individuals whose data is processed by our Academies.

The school DPCs report all data protection concerns to the central Data Protection Representative who liaises and works closely with the DPO.

The DPR/DPC contact details are as follows:

Waveney Valley Academies Trust	Sonia Parker	s.parker@waveneyvalleyat.co.uk
Sir John Leman High School	Donna Harmer	dxh@sirjohnleman.co.uk
Roman Hill Primary School	Laura Riley	l.riley@romanhill-pri.suffolk.sch.uk
Stowmarket High School	Michele Miall	m.miall@stowhigh.com
Alde Valley Academy	Liz Pattinson	headspa@aldevalley.suffolk.sch.uk
Northgate Primary School	Anita Smith	office@northgateprimary.norfolk.sch.uk
Southtown Primary School	Zoe Chilvers	office@southtown.norfolk.sch.uk

6. Privacy Notices

Waveney Valley Academies Trust and our Academies have a duty to check that staff, childrens', parents' and carers' information is accurate and up to date. It fulfils this by sending out a data collection form to parents/carers/staff on an annual basis.

This form will also include a privacy notice which outlines:

- who we are (including our contact details);
- the contact details of our Data Protection Officer;
- the purpose of the school processing data;

- the legal basis for processing data; and
- who this data will be shared with.

The current privacy notices for each relevant category of data subjects can be found on the Waveney Valley Academies Trust website and our Academies' websites.

7. Data Retention

The retention schedule can be found in the main offices at each location.

The retention schedule is based on guidance from the information and records management society: https://irms.org.uk/page/SchoolsToolkit and it encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

Waveney Valley Academies Trust will only process personal data where there is one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil/student) has freely given clear consent

For special categories of personal data, the processing must also meet one of the special category conditions which are set out in the GDPR and Data Protection Act 2018.

If the Trust offers online services to pupils/students, consent will be obtained, (except for online counselling and preventive services).

Whenever personal data is collected directly from individuals, the Trust will provide the relevant information required by data protection law.

8.2 Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons which will be explained to the individuals involved.

If the personal data is to be used for reasons other than those initially given, the Trust will inform the individuals concerned in advance, and consent will be sought where necessary. Staff must only process personal data where it is necessary in order to undertake their role.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be carried out in accordance with the retention schedule.

9. Sharing personal data

Waveney Valley Academies Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil/student or parent/carer that puts the safety of Trust staff at risk
- The Trust needs to liaise with other agencies – consent will be sought in advance, as necessary
- Trust suppliers or contractors need data to enable us to provide services to our staff and pupils/students – for example, IT companies. In such a situation, the Trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any shared personal data
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust

The Trust will also share personal data with law enforcement and government bodies where legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any Trust pupils/students or staff.

Where personal data is transferred to a country or territory outside the European Economic Area, the Trust will comply with data protection law.

10. Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Trust will advise them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the school has failed to comply with their data protection rights; and
- whether or not the school carries out automated decision-making and the logic involved in any such decision-making (i.e. e-recruitment software.)

The Trust will also provide the individual with a copy of the personal data being processed.

To make a subject access request, the individual should complete the relevant form and/or send a written request to the Academy DPC. In some cases, the school may need to ask for proof of identification before the request can be processed. The school will inform the individual if it needs to verify their identity and the documents it requires.

The Trust will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the school processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Academy will advise the individual, in writing, within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the school is not obliged to comply with it. Alternatively, the school can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Academy has already responded. If an individual submits a request that is unfounded or excessive, the Academy will notify them that this is the case and whether or not it will respond to it.

If a member of Trust staff receives a subject access request they must immediately forward it to the Academes DPC who will liaise with the Trust DPR in the first instance. Following this, contact will be made with the DPO as appropriate.

11. Other Rights

Individuals have a number of other rights in relation to their personal data. They can require the Academy to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the school's legitimate grounds for processing data (where the school relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the school legitimate grounds for processing data.

To ask the Academy to take any of these steps, the individual should send a written request to the Academy DPC.

12. Disclosure of Personal Information

Information sharing between professionals is vital to ensure the wellbeing of Children.

The school will follow the "7 golden rules of Information Sharing" described by the DfE:

- Remember that the DPA/GDPR is not a barrier to sharing information
- Be open and honest with the person or family
- Seek advice if you are in any doubt
- Share with consent where appropriate
- Consider safety and well-being
- Necessary, proportionate, relevant, accurate timely, and secure
- Keep a record of your decision and reasons

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

13. Access to Pupils Records

Parents have two distinct rights to access information about their child held by a school. These rights are:

- The parent's right of access to their child's educational record under The Education (Pupil Information) Regulations 2005. A link to this document can be found here. http://www.legislation.gov.uk/uksi/2005/1437/contents/made
- The pupil's right of subject access

A child or young person will always be the owner of their personal information. However, if a young person is incapable of making their own decisions, which is generally accepted as including children under the age of 12, the primary carer or guardian should act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

The Trust will respond to a subject access request within 1 calendar month. If this request comes from someone other than the data subject, the school will consider the suitability of the individual making the request and ensure that the sharing of information is in the best interests of the data subject.

Requests for information from pupils, or parents, for information that contains, wholly or partly, an educational record must receive a response within 15 school days.

14. Data Security

Waveney Valley Academies Trust and our Academies take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where Waveney Valley Academies Trust and our Academies engage third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

15. Waveney Valley Academies Trust use of Email

Waveney Valley Academies Trust and our Academies provide e-mail and internet access to authorised users. The use of email across the Trust is an essential means of communication for staff and students. In the context of the organisation, emails should not be considered private and individuals should assume that anything they write or email could become public.

Trust and Academy email accounts must be used for all business communication. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal contact information being revealed.

For the safety and security of users and recipients, all mail is filtered and logged.

The following rules will apply:

- Under no circumstances should personal email addresses be used for academy or Trust business.
- It is the responsibility of each account holder to keep their password(s) secure.
- Waveney Valley Academies Trust has a standard disclaimer to be attached to all email correspondence, clarifying that any views expressed are not necessarily those of the Trust. Please note that this disclaimer is automatically added to emails sent externally.

- All emails should be written and checked carefully before sending.
- All emails created or received may be subject to disclosure in response to a request for information under the Freedom of Information Act or a Subject Access Request in certain circumstances.

16. Emailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data without the use of encryption is strictly prohibited. Users should ensure that they have read and are aware of the policy.

Where the conclusion is that email should be used to transmit such data, caution will be exercised when sending the email and checks will be made before releasing the email:

- the details should be checked, including the accuracy of email addresses for recipient(s)
- Emails should not be copied or forwarded to any more recipients than is absolutely necessary.
- information should not be sent to any person whose details have not been verified.
- information should be sent as an encrypted/password protected document attached to an email wherever possible.
- encryption keys or password should be sent by a separate contact with the recipient(s)
- the identify of an individual or the nature of sensitive information should not be disclosed in the subject line of an email.
- confirmation of safe receipt should be requested

17. Privacy Impact Assessments

Some of the processing that the Waveney Valley Academies Trust and Academies within the Trust undertake may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Trust will carry out a data privacy impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

18. Data Breaches

Waveney Valley Academies Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

Any data breaches will be reported to the ICO within 72 hours. Examples of possible breaches in a multi academy trust context may include, but are not limited to:

- A non-anonymised dataset being published on a Trust or school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an electronic or data storage device containing non-encrypted personal data about pupils

19. Individual Responsibilities

Individuals are responsible for helping Waveney Valley Academies Trust and Academies within the Trust to keep their personal data up to date. Individuals should let the DPC within their Academy know if there have been any changes, for example if an individual moves house.

Staff members may have access to the personal data of other individuals in the course of their employment. Where this is the case, the Trust relies on its employees to meet its data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Trust) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Trust/Academies premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

20. Training

Waveney Valley Academies Trust will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

All staff are responsible for ensuring that information is managed according to this policy.