

## Data Protection Policy

|                              |   |
|------------------------------|---|
| <b>Policy Reference:</b>     | A65   |
| <b>Version Number:</b>       | 6   |
| <b>Applies to:</b>           | All services                                |
| <b>Associated documents:</b> | Data Retention Policy<br>Data Breach Policy |
| <b>Approved by:</b>          | Data Protection Committee                   |
| <b>Implementation date:</b>  | April 2026                                  |
| <b>Next review due by:</b>   | April 2027                                  |

# Aurora

## Contents

|  |    |
|--|----|
| Section 1 - Introduction and definitions .....                       | 3  |
| Section 2 – Data Protection Principles .....                         | 5  |
| Section 3 – Data Subject’s Rights and Requests .....                 | 11 |
| Section 4 - Accountability .....                                     | 12 |
| Section 5 – Automated Processing and Automated Decision Making ..... | 15 |
| Section 6 - Implementation of the policy and monitoring .....        | 15 |
| Appendix – Subject Access Requests .....                             | 17 |

## Section 1 - Introduction and definitions

### Introduction

The UK General Data Protection Regulation (UK GDPR), together with the Data Protection Act 2018 and the Data Use and Access Act 2025 (DUAA), provides the legal framework that governs how personal data must be collected, used, accessed, and protected within the United Kingdom. Collectively, these laws ensure a fair balance between an individual's right to privacy and the lawful, transparent, and responsible processing of personal data by organisations in the course of their business. They aim to safeguard the rights of individuals whose data is obtained, stored, processed, shared, or accessed, and require organisations to implement appropriate technical and organisational measures to prevent unauthorised access, alteration, disclosure, or destruction of personal data.

This policy sets out how the Aurora Group handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

The Aurora Group is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This policy does not form part of any individual's terms and conditions of employment with the Aurora Group and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Aurora Group's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

### Definitions: -

#### ***Personal Data***

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

# Aurora

## ***Special Category Data and Data Relating to Criminal Convictions and Offences***

Previously termed “Sensitive Personal Data”, Special Category Data is similar by definition and refers to data concerning an individual Data Subject’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data.

Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures

### ***Data Subject***

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

### ***Data Controller***

The organisation storing and controlling such information (i.e. the Aurora Group) is referred to as the Data Controller

### ***Processing***

Processing data is any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

### ***Automated Processing***

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

### ***Data Protection Impact Assessment (DPIA)***

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

### ***Data Breach***

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data.

# Aurora

## ***Pseudonymised***

The process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measure to ensure that the personal data cannot be attributed to an identifiable individual.

## ***Service/Business Function***

The Service refers to the school/college or residential home within the Aurora Group.  
The Business Function refers to the central service within the Aurora Group.

## **Section 2 – Data Protection Principles**

The Aurora Group are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the Aurora Group must adhere to are set out below.

### **Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner**

The Aurora Group only collect, process and share personal data fairly and lawfully and for specified purposes.

Before the processing starts for the first time, we will review the purposes of the processing activity and select the most appropriate lawful basis for that processing.

### ***Personal Data***

The Aurora Group may only process a data subject's personal data if one of the following fair processing conditions are met: -

- **Consent** — The data subject has given clear and unambiguous consent for their personal data to be processed for a specific purpose.
- **Contractual necessity** — The processing is necessary to perform a contract with the data subject, or to take steps at the data subject's request prior to entering into a contract.
- **Vital interests** — Processing is necessary to protect the vital interests of the data subject or another person.
- **Legal obligation** — Processing is necessary to comply with a legal obligation to which the Aurora Group is subject (other than contractual obligations).
- **Public task** — Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- **Legitimate interests** — Processing is necessary for the Aurora Group's legitimate interests where such interests are not overridden by the rights and freedoms of the data subject.
- **Recognised Legitimate Interests (new under DUAA 2025)** — The DUAA 2025 introduces a new lawful basis that allows certain processing for specified recognised legitimate interests such as crime prevention, safeguarding vulnerable people, emergency responses and national security without requiring an additional balancing test, provided the processing remains necessary for those purposes.

## **Special Category Data**

The Aurora Group may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- **Explicit Consent** — The data subject has given explicit, specific and informed consent to the processing for one or more specified purposes.
- **Employment, Social Security and Social Protection Law** — The processing is necessary for the purposes of carrying out obligations or exercising specific rights of the Service or the data subject in the field of employment law, social security law or social protection law, in accordance with applicable legislation. This may include (without limitation):
  - Managing sickness absence;
  - Assessing fitness to work and working capacity;
  - Making reasonable adjustments for disability;
  - Administering employee benefits (including private medical insurance);
  - Providing contractual or statutory sick pay;
  - Safeguarding and welfare responsibilities.
- **Vital Interests** — The processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.
- **Legal Claims and Compliance** — The processing is necessary for the establishment, exercise or defence of legal claims, or for compliance with a legal obligation imposed on the Aurora Group (other than a purely contractual obligation).
- **Data Made Public by the Data Subject** — The processing relates to personal data which has manifestly been made public by the data subject.
- **Substantial Public Interest** — The processing is necessary for reasons of substantial public interest, on the basis of UK law, including safeguarding children and vulnerable individuals, preventing or detecting unlawful acts, promoting equality of opportunity, or complying with regulatory requirements. Where required, an Appropriate Policy Document (APD) will be maintained in accordance with Schedule 1 of the Data Protection Act 2018 (as amended).
- **Preventive or Occupational Medicine and Health or Social Care Purposes** — The processing is necessary for preventive or occupational medicine, medical diagnosis, assessment of working capacity, provision of health or social care or treatment, or the management of health or social care systems and services, and is carried out by or under the responsibility of a health professional or another person subject to a duty of confidentiality.
- **Public Health** — The processing is necessary for reasons of public interest in the area of public health, including protecting against serious cross-border threats to health or ensuring high standards of quality and safety in healthcare.
- **Archiving, Research and Statistical Purposes** — The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to appropriate safeguards, including data minimisation and, where appropriate, pseudonymisation, in accordance with UK data protection legislation and the clarifications introduced under the Data (Use and Access) Act 2025.

# Aurora

The Aurora group identifies and documents the legal grounds being relied upon for each processing activity.

## **Consent**

Where the Aurora Group relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the Aurora Group will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The Services within the Aurora Group will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

## **Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes**

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The Aurora Group will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

## **Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

The Aurora Group will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the Aurora Group shall delete or anonymise the data.

[Please refer to the Data Retention Policy for further guidance].

## **Principle 4: Personal data must be accurate and, where necessary, kept up to date**

# Aurora

The Aurora Group will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Aurora Group.

**Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed**

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Aurora Group will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is store and how that period is determined in our privacy notices.

Please refer to the Retention Policy for further details about how the Aurora Group retains and removes data.

**Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage**

To assure the protection of all data being processed, the Aurora Group will develop, implement and maintain reasonable safeguards and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where Aurora replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.
- Ensuring personal data is not entered into an unauthorised AI tool (see below);

The Aurora Group follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Aurora Group will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place. (see below)

# Aurora

The Aurora Group will only transfer data outside the European Economic Area if the appropriate safeguards are in place. (see below)

Full details on the Aurora Group's IT security measures are set out in the IT Acceptable Use Policy. All employees are obligated to follow these policies. (see below)

## ***Sharing Personal Data***

The Aurora Group will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the Aurora Group is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the department of health/education. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the Aurora Group shall be clearly defined within written notifications including details and the basis for sharing the data.

## ***International Transfers of Personal Data***

The Aurora Group will not transfer personal data outside the United Kingdom unless the transfer complies with UK GDPR as amended by the Data (Use and Access) Act 2025. A restricted transfer includes sending, storing or allowing access to personal data from outside the UK. Transfers will only take place where the destination is subject to UK adequacy regulations or where appropriate safeguards are in place, such as an International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, Binding Corporate Rules, or another lawful mechanism recognised under UK law. Where required, a documented transfer risk assessment will be undertaken. Staff must comply with the Aurora Group's procedures before any international transfer occurs.

## ***Employee Obligations***

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Aurora Group in the course of their employment or engagement. If so, Aurora

# Aurora

expects those employees to help meet the Aurora Group's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to service premises, computer access, password protection and secure file storage and destruction [Please refer to the Acceptable Use Policy for further details about our security processes];
- Not remove personal data or devices containing personal data from Aurora premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;

## ***Artificial Intelligence (AI)***

Artificial intelligence (AI), including generative AI tools and chatbots, is increasingly accessible within the workplace. The Aurora Group recognises that the use of such tools may involve the processing of personal data and, in some cases, special category data.

To protect individuals' rights and freedoms and to comply with UK data protection law, employees must not input, upload or otherwise disclose personal data or special category data into any unauthorised AI system, generative AI tool or external chatbot.

Use of AI systems that process personal data is only permitted where:

- The tool has been formally approved by the Aurora Group;
- A lawful basis for processing has been identified;
- A risk assessment (and, where required, a Data Protection Impact Assessment) has been completed;
- Appropriate contractual, technical and organisational safeguards are in place; and
- The use complies with the organisation's data protection, confidentiality and information security policies.

Where AI is used to support decision-making that may have legal or similarly significant effects on individuals, the Aurora Group will ensure compliance with the safeguards relating to automated decision-making under UK GDPR, as clarified by the Data (Use and Access) Act 2025, including transparency, meaningful human oversight where required, and the ability for individuals to challenge decisions.

Any employee who enters personal or special category data into an unauthorised AI tool will be considered to have committed a potential personal data breach. Such incidents will be managed in accordance with the Aurora Group's Data Breach Policy and may result in disciplinary action.

## Section 3 – Data Subject’s Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Aurora Group handle their personal data are set out below: -

- (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
  - Receive certain information about the Aurora Group’s processing activities;
  - Request access to their personal data that we hold (see “Subject Access Requests” Appendix);
  - Prevent our use of their personal data for marketing purposes (see below);
  - Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
  - Restrict processing in specific circumstances;
  - Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
  - Request a copy of an agreement under which personal data is transferred outside of the EEA;
  - Object to decisions based solely on automated processing;
  - Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
  - Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
  - Make a complaint to the supervisory authority; and
- (a) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Service to verify the identity of the individual making the request and respond without delay and within one calendar month of receipt of the request (or receipt of the additional information needed to confirm identity or clarify the request). The time period for responding to a SAR may be extended by a further two months if the request is complex.

### Direct Marketing

The Aurora Group are subject to certain rules and privacy laws when marketing. For example, a data subject’s prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Aurora Group will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand and promptly respond to any individual objection to direct marketing.

### Requests for Educational Record

Parents, or those with parental authority, have a legal right to free access to their child’s educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

# Aurora

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

## Data Protection Complaints

Individuals have the right to raise concerns or complaints about how their personal data is handled.

All data protection complaints must be submitted and managed through the Aurora Group Complaints Policy, which provides the organisation's formal complaints procedure and escalation framework.

Where a complaint relates to data protection, it will:

- be referred to the Data Protection Officer (DPO);
- be assessed to determine whether it constitutes a personal data breach or rights request;
- be investigated in accordance with this policy and relevant data protection procedures.

Further guidance for staff on handling data protection complaints is set out in Appendix 2.

## Section 4 - Accountability

The Aurora Group will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The Aurora Group have taken the following steps to ensure and document UK GDPR compliance: -

### Appointment of a Data Protection Officer (DPO)

The Aurora Group has appointed **Marie Turner** as Data Protection Officer (DPO). The DPO is responsible for overseeing the implementation of this Policy, developing data-related policies and guidelines, and ensuring compliance with UK data protection law, including obligations introduced by the DUAA 2025.

Staff must contact the DPO in the following circumstances:

- Uncertainty about the lawful basis for processing personal data;
- Reliance on consent as a basis for processing;
- Drafting privacy notices or fair processing information;
- Clarification of retention periods for personal data;
- Questions regarding appropriate security measures;
- Suspected or actual personal data breaches;
- Transfers of personal data outside the UK;
- Exercising or responding to data subject rights;
- Planning significant new or amended processing activities that may require a **Data Protection Impact Assessment (DPIA)**;
- Use of automated processing or automated decision-making, including AI tools;
- Compliance with direct marketing requirements;
- Sharing personal data with third parties under contracts or other arrangements.

## **Personal Data Breaches Notification**

The data protection legislation requires the Aurora Group to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches and your DPO.

[Please refer to the Data Breach Policy for further guidance].

## **Transparency and Privacy Notices**

The Aurora Group will provide detailed, specific information to data subjects. This information will be provided through the Aurora privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The Aurora privacy notices are tailored to suit the data subject and set out information about how the Aurora Group will use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR, the DPA 2018 and DUAA 2025. This includes the identity of the Data Protection Officer and how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The Aurora Group will also confirm whether that third party has collected and processed data in accordance with the data protection legislation.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

## **Privacy by Design and Default approach to Data Protection**

The Aurora Group adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Aurora Group takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

# Aurora

## Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Aurora Group conduct DPIAs for any new technologies or programmes being used by the Services which could affect the processing of personal data. In any event, the Aurora Group will carry out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs detail the following: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

## Record Keeping

The Services are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the Service;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the Service's processing activities and purposes;
- Details of any third-party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

## Training

The Services / Business Functions across the group will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. All staff complete data protection training as part of their induction process and data protection will form part of continuing professional development. An accurate data protection training log is kept by each service/function.

## Data Audit Implementation

The Services, through the Data Protection Officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly to review use of personal data.

## Section 5 – Automated Processing and Automated Decision Making

### Overview

The Aurora Group does not routinely make decisions about pupils, parents, carers or staff based solely on automated processing.

Where automated tools (e.g. safeguarding systems, attendance monitoring, behaviour tracking, assessment analytics or HR screening tools) are used, meaningful human oversight will always be applied.

A solely automated decision that produces legal or similarly significant effects will only take place where permitted by law and with appropriate safeguards.

### Lawful Basis

Solely automated decision-making with legal or similarly significant effects will only occur where:

- The individual has given explicit consent;
- The processing is authorised by law; or
- The processing is necessary for entering into or performing a contract.

Where special category data (including health or SEND-related data) is involved, such processing will only occur where there is explicit consent or a clear statutory basis, and where substantial public interest conditions are met where required.

### Safeguards for Pupils and Staff

Where relevant, The Aurora Group will:

- Inform individuals if a significant decision is based solely on automated processing;
- Provide clear information about the logic involved and the likely consequences;
- Offer the right to request human intervention;
- Allow individuals to express their view and challenge the decision.

### DPIA and Governance

Before introducing any high-risk automated processing (particularly involving children, safeguarding data, health information or behavioural profiling), The Aurora Group will conduct and document a Data Protection Impact Assessment (DPIA);

Automated systems will be reviewed periodically to ensure accuracy, fairness and continued compliance.

## Section 6 - Implementation of the policy and monitoring

This Policy shall be deemed effective from April 26. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

### Related Policies

Staff should refer to the following policies that are related to this Data Protection Policy: -

# Aurora

1. Data Breach Policy, Data Retention Policy, Information Governance Policy, Acceptable Use Policy.
2. These policies are also designed to protect personal data and can be found on SharePoint under Group Policies

## Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Aurora Group.

# Aurora

## Appendix 1 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the Aurora Group hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the Aurora Group are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under Data Protection Law puts both staff and the Aurora Group at potentially significant risk and so the Aurora Group takes compliance with this policy very seriously.

A data subject has the right to be informed of the following: -

1. Confirmation that their data is being processed;
2. Access to their personal data;
3. A description of the information that is being processed;
4. The purpose for which the information is being processed;
5. The recipients/class of recipients to whom that information is or may be disclosed;
6. Details of the sources of information obtained;
7. In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
8. Other supplementary information.

### How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Aurora Group process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text, via social media accounts) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the school hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

## How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the Aurora Group to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

Aurora encourages the use of [dpo@the-aurora-group.com](mailto:dpo@the-aurora-group.com) for making data subject requests, although it recognises the right of individuals to make requests through any available route. Aurora cannot refuse to deal with a request if it does not use the preferred route, nor require the data subject to resubmit the request.

## What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed, in the first instance, to your line Manager. The Service will nominate a SAR Lead who will record the details of the request on GDPR Sentry for automatic referral to the Data Protection Officer who together with the Data Protection Team can assist with the request and review what is required.

There are limited timescales within which Aurora must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

This being the case, the delivery of subject access requests needs to be managed by staff who are able to collect appropriate data without administrative delay: -

- The Aurora Data Protection Team comprises a permanent core team, supplemented by other members depending on the nature of the request being managed. Whilst the core team will advise, guide and support, collating and checking the information requested, will be managed at service or function level.
- The Data Protection Team is coordinated by the Quality and Governance Co-ordinator and includes The Data Protection Officer.
- The team will reflect representation of the major functions within The Aurora Group (Senior Leadership, Teaching and Learning, Administration, and IT). Service and function staff will be instructed and supported in responding to the request but must identify who will own and process the SAR as soon as practicable after receiving the request.

## Acknowledging the Request

When receiving a SAR, the Aurora Group shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the Service/Function may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the Service must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

# Aurora

The Service/Function under the guidance of the DPO will prepare an appropriate acknowledgment and ensure it is sent to the requestor within 3 days of receipt of the SAR.

## Verifying the Identity of a Requester

Before responding to a Subject Access Request (SAR), the relevant Service/Function will take reasonable and proportionate steps to verify the identity of the person making the request.

For current employees, this will usually be straightforward. However, The Aurora Group is entitled to request additional information where necessary to confirm that the requester is the data subject (or is authorised to act on their behalf).

Where there are reasonable doubts as to identity, appropriate evidence may be requested, such as:

- Passport;
- Driving licence;
- Recent utility bill confirming current address;
- Birth or marriage certificate;
- Credit card or mortgage statement; or
- Other suitable official documentation.

The level of verification requested will be proportionate to the sensitivity of the personal data involved.

## Clarification of Requests

Where a request is unclear or relates to a large volume of information, the Service/Function may ask the requester to clarify the scope of the request in order to locate the relevant data efficiently.

The requester will **never** be asked to explain the reasons for making the request.

The Service/Function, under the guidance of the Data Protection Officer (DPO), will contact the requester as soon as possible if:

- Additional identity verification is required; or
- Clarification of the scope of the request is necessary.

## “Stop the Clock” Provision

In accordance with the Data (Use and Access) Act 2025, where The Aurora Group:

- Reasonably requires further information to verify identity; or
- Requires clarification to identify the personal data requested,

the statutory time limit for responding to the SAR will be **paused (“stopped”)** from the date the request for additional information is issued until the requested information is received.

The response period will recommence once sufficient information has been provided.

# Aurora

If the requester does not provide the additional information reasonably required to verify identity or clarify the request, The Aurora Group may be unable to proceed with the request.

## **Requests Made by Third Parties or on Behalf of Children**

The Aurora Group need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The Aurora Group may also require proof of identity in certain circumstances.

If the Aurora Group is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Given the cohort at the Aurora Group, special attention must be paid to any requests coming from parents of students or residents for information about the child/young person. Before responding to a SAR for information held about a child, the Service should consider whether the child is mature enough to understand their rights.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, provided that the Service is confident that the young person understands their rights and there is no reason to believe that the young person does not have the capacity to make a request on their own behalf, then the Service should usually respond directly to the child/young person or seek their consent before releasing their information. Special care will need to be taken, and each request considered on a case-by-case basis.

The Service may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

## **Fee For Responding to a SAR**

The Aurora Group will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive, a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the Service/Function under the guidance of the DPO will inform the requester why this is

# Aurora

considered to be the case, and that the Aurora Group will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

## **Time Period for Responding to a SAR**

The Aurora Group has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where there is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third-party requester, the written authorisation of the data subject has been received. The clock may be stopped if further clarification is required until such clarification has been given.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Aurora Group will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

## **Service Closure Periods**

During school and college closure periods, the Group's ability to respond to data protection requests may be affected. Requests received during, or shortly before, a closure period may not be acknowledged or processed within the standard one calendar month timeframe, due to reduced staffing levels and limited access to necessary systems.

While the Group will acknowledge requests where possible, full processing may be delayed until normal operations resume. The Group will endeavour to comply with statutory response times and will maintain communication where reasonably practicable.

To help avoid delays, individuals are encouraged to submit urgent data protection requests during term time and outside of known closure periods.

## **Information to be Provided in Response to a Request**

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular, where those recipients are in third countries or international organisations;

# Aurora

- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right: -
  - to request that the Company rectifies, erases or restricts the processing of his personal data; or
  - to object to its processing;
  - to lodge a complaint with the ICO;
  - where the personal data has not been collected from the individual, any information available regarding the source of the data;
  - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the Aurora Group are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Aurora Group have one month in which to respond the Aurora Group is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the Aurora Group is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Aurora Group is not allowed to amend or delete data to avoid supplying the data.

The information will be provided to the requester in the appropriate format by the Service/Function under the guidance of the DPO.

## How to Locate Information

The personal data the Aurora Group need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Aurora Group may need to search all or some of the following:

- electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The Aurora Group should search these systems using the individual's name, employee number or other personal identifier as a search determinant. The search will be co-ordinated by the Data Protection Team under the guidance of the Data Protection Officer.

## Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case-by-case basis.

The Aurora Group will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the Aurora Group do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless: -

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all the relevant circumstances will be considered, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual can give consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Aurora Group disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the Aurora Group must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

## Other Exemptions to the Right of Subject Access

In certain circumstances the Aurora Group may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

*Crime detection and prevention:* The Aurora Group do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

*Confidential references:* The Aurora Group do not have to disclose any confidential references given to or received from third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

*Legal professional privilege:* The Aurora Group do not have to disclose any personal data which is subject to legal professional privilege.

*Management forecasting:* The Aurora Group do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

*Negotiations:* The Aurora Group do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

# Aurora

*Potential for Harm:* The Aurora Group do not have to disclose any personal data which may cause serious harm to the physical or mental health of a pupil, resident or another individual.

## **Refusing to Respond to a Request**

The Aurora Group can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the Aurora Group can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the Aurora Group need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the Aurora Group should contact the individual promptly and inform them. The Aurora Group do not need to comply with the request until the fee has been received.

In some cases, where the task of redaction is unfeasible (most often with CCTV footage) a decision may be made that the information cannot be released even though it represents personal data of that data subject. In some cases, other policies will override the data protection policy in respect of releasing information. This is especially the case with safeguarding information. Where data is redacted or withheld, a record should be added to the log of the request.

## **Record Keeping**

A record of all subject access requests shall be kept by the DPO on the central Subject Access Request Log. The record shall include the date the SAR was received, the name of the requester, what data the Aurora Group sent to the requester, the rationale for withholding data, and the date of the response.

## Appendix 2 – Data Protection Complaints

Under data protection law, individuals have the right to raise concerns or make complaints regarding the handling of their personal data.

All complaints must be raised and managed in accordance with the Aurora Group Complaints Policy, which provides the formal process for complaint handling and escalation.

This appendix sets out additional requirements for the identification, escalation, and handling of data protection complaints, to ensure compliance with legal and regulatory obligations.

The Aurora Group treats all data protection complaints seriously. Failure to address such complaints appropriately may result in regulatory action and reputational risk.

### What is a Data Protection Complaint?

A data protection complaint is any expression of dissatisfaction relating to how the Aurora Group processes personal data or responds to a data protection request.

Examples include complaints about:

- inaccurate, incomplete, or outdated personal data;
- personal data being processed without a lawful basis;
- failure to respond to a data subject rights request;
- unauthorised disclosure or loss of personal data;
- lack of transparency in data processing activities; or
- any other potential breach of data protection legislation.

A complaint does not need to refer specifically to “data protection” or “UK GDPR” to be treated as such.

### How to Make a Data Protection Complaint

Complaints must be submitted using the routes set out in the Aurora Group Complaints Policy. An informal complaint may be made verbally or in writing.

The formal stage involves the complainant putting the complaint into writing by email or letter.

Where a complaint relates wholly or partly to personal data, it must be identified as a data protection complaint and escalated internally to the Data Protection Officer (DPO).

### Acknowledging and Investigating a Complaint

All complaints will be acknowledged and managed in accordance with the timescales set out in the Complaints Policy.

Where a complaint relates to data protection:

- the Data Protection Officer (DPO) will be notified;
- the organisation will assess whether the matter constitutes a personal data breach;

# Aurora

- the organisation will assess whether the complaint includes or should be treated as a data subject rights request.

Where statutory obligations apply under data protection law, these will be complied with alongside the complaints process.

Investigations will be conducted in a timely, fair, and proportionate manner in accordance with the timescales set out in the Complaints Policy. This may include:

- reviewing relevant records and systems;
- consulting with relevant staff or departments; and
- seeking advice from the Data Protection Officer.

## Outcome of a Complaint

Following investigation, the Aurora Group will provide a written response setting out:

- the findings of the investigation;
- any actions taken or proposed; and
- details of the right to escalate to a review panel hearing if the complainant is not satisfied with the response to the stage 2 complaint.

If the complainant remains dissatisfied following completion of the Aurora Group's complaints procedure, they have the right to refer the matter to the Information Commissioner's Office (ICO).

The ICO is the UK's independent authority for upholding information rights.

For more information or to make a complaint, please visit:

<https://ico.org.uk/make-a-complaint>

## Complaints Received During Closure Periods

The Aurora Group will make reasonable efforts to acknowledge and investigate complaints as soon as practicable.

Where a complaint is received during a period of service closure or reduced operation, there may be delays in responding. In such cases, the complaint will be acknowledged and progressed as soon as reasonably practicable following the resumption of normal operations.

## Record Keeping

A record of all data protection complaints will be maintained, including:

- the date of receipt;
- the nature of the complaint;
- key actions taken during the investigation; and
- the outcome.

# Aurora

Records will be retained securely in accordance with the Aurora Group Records Retention Schedule.

## **Data Protection Complaint Form**

You can use this form to raise a concern or complaint about how the Aurora Group has handled your personal data.

There is no requirement to use this form. Complaints may also be made using the routes set out in the Aurora Group Complaints Policy.

Using this form may help us to understand and investigate your concerns more efficiently.

Completed forms should be submitted via the routes set out in the Complaints Policy (e.g. in writing by email or letter).

## **Proof of Identity**

Where a complaint relates to personal data, we may need to verify your identity before progressing the matter. Acceptable documents may include a passport or driving licence.

## Data Protection Complaint Form

### Section 1 – Your Details

Title:

Full Name:

Date of Birth:

Address:

Postcode:

Telephone Number:

Email Address:

### Section 2 – Details of Your Complaint

Please describe your concern in as much detail as possible, including relevant dates, names, and any supporting information.

(Use additional pages if required)

Have you previously raised this concern with the Aurora Group?

Yes  No

If yes, please provide details:

What outcome are you seeking?

### Section 3 – Representative Details (if applicable)

If you are making this complaint on behalf of someone else, please complete this section.

Full Name:

Address:

Postcode:

Telephone Number:

Email Address:

Relationship to the individual:

Proof of Authorisation:

# Aurora

- Written authority
- Power of Attorney
- Parental responsibility
- Other (please specify):

## Section 4 – Declaration

- I confirm that the information provided is accurate to the best of my knowledge.
- I understand that the Aurora Group may contact me to clarify details and verify my identity before investigating this complaint.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_