New Direction School

Data Protection Policy

Reviewed Date:	Reviewed By	List of changes	Next Review
August 2021	Luke Collins	• Reviewed with guidance from Andrew Howard	August 2022
July 2022	Luke Collins	• Reviewed with no changes needed	July 2023
July 2023	Luke Collins	• Reviewed with no changes needed	July 2024
October 2024	Adrian anderson	• Reviewed with no changes needed	October 2025
April 2026	Luke Collins	Fully reviewed and updated in line with UK GDPR, Data Protection Act 2018, DfE data protection guidance, KCSIE 2025, Working Together to Safeguard Children 2026, Independent School Standards guidance, current school roles, Arbor, CPOMS and safeguarding information-sharing expectations.	April 2027

Contents

1. Introduction

New Direction School aims to ensure that all personal data collected about pupils, parents and carers, staff, visitors, contractors, proprietors, volunteers and other individuals is collected, stored, shared and processed lawfully, fairly, transparently and securely.

This policy applies to all personal data processed by the school, whether held electronically, in paper format, in photographs or video, in emails, in school systems, or in any other form.

This policy supports the school's safeguarding, welfare, education, employment, contractual and statutory responsibilities. It should be read alongside the safeguarding and child protection policy, staff code of conduct, online safety policy, records retention schedule, privacy notices, exams policy, acceptable use arrangements and relevant procedures for Arbor, CPOMS and other school systems.

For the purposes of this policy, the term "pupil" includes all pupils and students on roll or receiving provision from the school.

2. Legislation and guidance

This policy has been written with regard to:

• UK General Data Protection Regulation (UK GDPR)

• Data Protection Act 2018

• Privacy and Electronic Communications Regulations, where relevant

• Education (Pupil Information) (England) Regulations 2005, where applicable to the school

• DfE Data Protection in Schools guidance and toolkit

• Information Commissioner's Office (ICO) guidance for organisations and schools

• Keeping Children Safe in Education 2025

• Working Together to Safeguard Children 2026

• Information Sharing: Advice for Practitioners Providing Safeguarding Services

• The Education (Independent School Standards) Regulations 2014 and Independent School Standards guidance

• JCQ and awarding body requirements relating to examination data, where applicable.

Data protection law does not prevent the school from sharing information where this is necessary to safeguard or promote the welfare of a child. The school will not allow concerns about consent or data protection to prevent appropriate safeguarding information sharing.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include names, initials, identification numbers, location data, online identifiers, pupil records, contact details, images, attendance information, behaviour information, safeguarding records, assessment information and any other information that can identify a person directly or indirectly.
Special category personal data	More sensitive personal data requiring additional protection. This includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics used for identification, health, disability, sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences, allegations, proceedings, related security measures, cautions or other disposals.
Processing	Anything done to personal data, including collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, sharing, disclosing, restricting, erasing or destroying it. Processing may 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 means of processing personal data.
Data processor	A person or organisation, other than an employee of the controller, that

	processes personal data on behalf of the 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.
Data Protection Impact Assessment (DPIA)	A process to identify and reduce data protection risks where processing is likely to result in a high risk to individuals' rights and freedoms.

4. The data controller

New Direction School processes personal data relating to pupils, parents and carers, staff, visitors, contractors, volunteers and others. The school is therefore a data controller for the personal data for which it determines the purposes and means of processing.

Where the school uses third-party systems or suppliers to process personal data on its behalf, those organisations will usually act as data processors. Where another organisation independently determines the purposes and means of processing, it may act as a separate controller or joint controller.

5. Roles and responsibilities

This policy applies to all staff employed by the school and to external organisations or individuals working on behalf of the school. Failure to comply with this policy may result in disciplinary action, contract review or other appropriate action.

5.1 The Proprietor

The Proprietor, Yvonne Evans, has overall responsibility for ensuring that the school complies with all relevant data protection obligations and that appropriate systems, policies and oversight arrangements are in place.

5.2 Directors and senior leaders

The Directors are Luke Collins and Hannah Oliver. The Head of Education is Luke Collins. The Head of Equine Provision is Hannah Oliver. Senior leaders are responsible for ensuring that staff understand and implement this policy in day-to-day practice.

5.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for advising the school on data protection compliance, monitoring implementation of this policy, supporting DPIAs, advising on data subject rights and acting as a contact point for individuals and the ICO.

The school's DPO is Luke Collins and is contactable via luke@new-direction.org.uk or 01246 810456.

The school will ensure that the DPO is able to act independently when carrying out DPO functions. Where the DPO is personally involved in a processing decision, safeguarding decision, breach, complaint, SAR or other matter that may create a conflict of interest, the Proprietor will arrange independent advice or oversight as appropriate.

5.4 Designated Safeguarding Lead and deputy DSLs

The DSL is Luke Collins. Deputy DSLs are Hannah Oliver, Emily Smith and Nikki Morris. The DSL and deputy DSLs are responsible for ensuring that safeguarding information is recorded, stored, shared and transferred securely and appropriately in line with KCSIE, Working Together and the school's safeguarding procedures.

5.5 All staff

All staff are responsible for:

• collecting, storing, using and sharing personal data only where required for their role and in line with this policy;

• keeping personal data accurate, secure and confidential;

• using Arbor, CPOMS, email, shared drives and other school systems appropriately and securely;

• not sharing passwords or allowing unauthorised access to school systems;

• informing the school of changes to their own personal data;

• forwarding all data protection rights requests immediately to the DPO;

• reporting any actual or suspected data breach immediately and no later than the same working day;

• contacting the DPO if they are unsure about lawful basis, consent, privacy notices, retention, third-party sharing, international transfers, DPIAs, data security or contracts involving personal data.

6. Data protection principles

The UK GDPR is based on data protection principles. The school will ensure that personal data is:

• processed lawfully, fairly and transparently;

• collected for specified, explicit and legitimate purposes;

• adequate, relevant and limited to what is necessary;

• accurate and, where necessary, kept up to date;

• kept for no longer than is necessary;

• processed securely using appropriate technical and organisational measures;

• processed in a way that allows the school to demonstrate accountability.

The school will maintain appropriate records, policies, procedures, privacy notices, contracts, retention information, training records and breach logs to demonstrate compliance.

7. Collecting and using personal data

7.1 Lawfulness, fairness and transparency

The school will only process personal data where it has a lawful basis under UK GDPR. The lawful bases most commonly used by the school include:

• compliance with a legal obligation;

• performance of a task carried out in the public interest or in the exercise of official authority, where applicable;

• performance of a contract or steps prior to entering a contract;

• protection of vital interests;

• legitimate interests pursued by the school or a third party, where those interests are not overridden by the rights and freedoms of the individual;

• consent, where this is appropriate and freely given.

For special category personal data, the school will also identify a relevant Article 9 condition and, where required, a Data Protection Act 2018 Schedule 1 condition. These may include employment, social security and social protection, health or social care, substantial public interest, safeguarding of children and individuals at risk, legal claims, vital interests or explicit consent.

For criminal offence data, the school will identify both a lawful basis and an appropriate condition under the Data Protection Act 2018.

Where the school collects personal data directly from individuals, it will provide privacy information explaining how and why the data is used, who it may be shared with, retention periods and individual rights. Privacy notices will be kept under review.

7.2 Limitation, minimisation and accuracy

The school will only collect personal data for specified, explicit and legitimate reasons. Staff must only process personal data where it is necessary for their role and must not access records without a legitimate work-related reason.

The school will take reasonable steps to keep data accurate and up to date. Inaccurate data will be corrected or erased where appropriate. Where data is no longer required, it will be securely deleted, anonymised or destroyed in accordance with the school's records retention schedule.

7.3 Key school systems

The school uses Arbor as its management information system to record pupil data, attendance and behaviour information. CPOMS is used to record safeguarding and child protection concerns. Access to these systems is restricted according to role and operational need.

Staff must ensure that information recorded on school systems is factual, proportionate, accurate, timely and relevant. Safeguarding records must be made and managed in accordance with the school's safeguarding and child protection policy.

8. Sharing personal data

The school will share personal data where there is a lawful basis for doing so and where sharing is necessary, proportionate and secure. The school may share information with parents and carers, local authorities, safeguarding partners, other schools, alternative providers, health services, social care, police, awarding bodies, DfE, Ofsted, professional advisers, insurers, payroll and pension providers, IT providers and other relevant organisations where appropriate.

8.1 Safeguarding and welfare information sharing

Data protection law does not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. The school will share information without consent where this is necessary and lawful for safeguarding, child protection, early help, welfare or emergency purposes.

It is not usually necessary to seek consent to share personal information for safeguarding purposes. The DSL or deputy DSL will decide whether safeguarding information needs to be shared and will ensure that the decision is recorded, including what was shared, with whom, when, why, the lawful basis and whether consent was sought or not sought.

Where possible and appropriate, the school will be open and transparent with pupils and families about information sharing. However, the school will not seek consent, or will not inform individuals before sharing, if doing so would place a child or another person at increased risk of harm, prejudice an investigation, prevent the detection or prevention of crime, or otherwise be inappropriate.

8.2 Sharing with suppliers and contractors

When using suppliers or contractors to process personal data, the school will:

• carry out appropriate due diligence;

• only use providers that give sufficient guarantees about data protection and security;

• ensure appropriate contracts or data processing agreements are in place;

• share only the personal data necessary for the service;

• review high-risk processing arrangements periodically;

• ensure international transfers are protected by appropriate safeguards where relevant.

8.3 Local authorities and multi-agency working

The school is based in Derbyshire and also works with Nottinghamshire, Rotherham and Sheffield local authorities. The school will share relevant information with local authorities, safeguarding partners and other agencies where required for education,

SEND, attendance, safeguarding, welfare, admissions, transitions, commissioning, funding, legal compliance or child protection purposes.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have the right to make a subject access request (SAR) to access personal data that the school holds about them. This includes confirmation that their personal data is being processed and access to a copy of the data, subject to exemptions and the rights of others.

Subject access requests can be made verbally or in writing. Staff who receive a request must immediately forward it to the DPO. The school may ask for clarification or identification where necessary.

A response will normally be provided without undue delay and within one month of receipt of the request or confirmation of identity, where required. Where a request is complex or numerous, the school may extend the response period by up to two further months and will explain this within one month.

The school will not normally charge a fee. A reasonable fee may be charged, or the request refused, where a request is manifestly unfounded or excessive.

9.2 Children and subject access requests

Personal data about a child belongs to that child, not to the child's parents or carers. Where a parent or carer makes a SAR for information about their child, the school will consider whether the child has sufficient understanding to exercise their own rights or consent to the request.

Children aged 12 and above are generally considered more likely to have sufficient understanding, but this will always be assessed case by case. As many pupils at New Direction have additional needs, competence must not be assumed and must be considered carefully, taking into account the pupil's age, understanding, needs, wishes and best interests.

9.3 Information that may be withheld

The school may withhold information where an exemption applies, including where disclosure would:

• cause serious harm to the physical or mental health of a pupil or another individual;

• reveal that a child is being, has been or may be at risk of abuse where disclosure would not be in the child's best interests;

• disclose another person's personal data and it would not be reasonable to disclose it;

• prejudice crime prevention or detection, legal proceedings, legal advice, regulatory activity or safeguarding activity;

• disclose confidential references, management information, negotiations, examination scripts or other exempt information.

Where the school refuses a request in whole or in part, it will explain why, unless doing so would undermine the purpose of the exemption, and will inform the individual of their right to complain to the ICO or seek enforcement through the courts.

9.4 Other data protection rights

Individuals may also have the right to:

• be informed about how their data is used;

• have inaccurate data rectified;

• request erasure of personal data in certain circumstances;

• request restriction of processing in certain circumstances;

• object to processing in certain circumstances;

• withdraw consent where processing is based on consent;

• data portability in certain circumstances;

• object to direct marketing;

• challenge solely automated decisions or profiling with legal or similarly significant effects;

• be notified of certain personal data breaches;

• complain to the ICO.

Requests to exercise these rights should be forwarded immediately to the DPO.

10. Parental requests to see the educational record

Parents or those with parental responsibility may request access to their child's educational record. Where the Education (Pupil Information) (England) Regulations 2005 apply to the school, the school will respond within 15 school days of receiving a written request, subject to relevant exemptions.

Where those regulations do not apply to the school's legal category or to the specific request, the school will consider the request under UK GDPR subject access rights and any other applicable legal duties.

The school may refuse or limit access where disclosure would cause serious harm to the physical or mental health of the pupil or another person, disclose information about another person, reveal safeguarding concerns where this would not be in the child's best interests, or disclose exam marks before official publication.

11. Photographs and videos

As part of school life, the school may take photographs or videos of pupils, staff and visitors. Images may be used for identification, learning activities, assessment, displays, newsletters, the school website, social media, communication with families, promotional material or evidence of provision, depending on the purpose and lawful basis.

The school will obtain written consent from parents and carers for photographs and videos of pupils where consent is the appropriate lawful basis. Additional consent will be sought for communication, marketing or promotional uses where required. The school will also consider the wishes and understanding of pupils.

Consent can be refused or withdrawn at any time. Where consent is withdrawn, the school will stop further use of the image where consent was the lawful basis and will take reasonable steps to remove it from school-controlled platforms.

The school will not publish images in a way that creates an avoidable safeguarding risk. Particular care will be taken for looked-after children, previously looked-after children, children subject to safeguarding plans or any pupil where there are known safety concerns.

Staff must not use personal devices to take or store images of pupils unless specifically authorised for a legitimate school purpose and in line with school procedures. Images must be transferred to secure school systems and deleted from personal devices as soon as practicable.

Parents and carers taking photographs or videos at school events for personal use are not covered by data protection legislation. However, the school will ask that images or videos containing other pupils are not shared publicly, including on social media, unless the relevant parents/carers or pupils where appropriate have agreed.

12. Examination data

The delivery of examinations and assessments involves the processing of personal data by the school, awarding bodies, JCQ and other relevant organisations. The school will process examination data in accordance with UK GDPR, the Data Protection Act 2018, JCQ requirements and awarding body instructions.

Examination-related data may include candidate details, entries, access arrangements, special consideration requests, attendance at examinations, conduct records, non-examination assessment information, results, post-results services, appeals and certificates.

Candidate examination data may be shared with awarding bodies, JCQ, the Department for Education, local authorities and other organisations where required for the administration and integrity of examinations and assessments.

Candidates will be made aware of relevant privacy information, including the JCQ Information for Candidates - Privacy Notice. Where access arrangements require awarding body approval, candidates will be asked to complete the relevant JCQ data protection and consent documentation where required.

Requests for examination information should be made to the DPO. If a request is made before exam results have been published, the school will respond within the statutory timescales applicable to examination data. If a request is made after publication of results, the school will respond within one month unless an extension or exemption applies.

The school will not publish examination results in a way that breaches data protection law, safeguarding expectations or the reasonable wishes and rights of candidates.

13. Data protection by design and default

The school will integrate data protection into its processing activities by:

• appointing a DPO and ensuring appropriate data protection oversight;

• using privacy notices to explain how personal data is used;

• maintaining records of processing activities and a data asset register where appropriate;

• conducting DPIAs where processing is likely to result in high risk to individuals;

• considering privacy and security before introducing new systems, technology, apps, software, contracts or processing activities;

• limiting access to personal data according to role and need;

• reviewing data retention and deletion arrangements;

• training staff and keeping training records;

• reviewing data processors and data sharing arrangements;

• keeping policies, procedures and privacy information under regular review.

A DPIA will be considered for new or changed processing involving large-scale special category data, safeguarding systems, monitoring, biometrics, new technology, profiling, automated decision-making, high-risk data sharing or any activity likely to affect individuals' rights and freedoms.

14. Data security and storage of records

The school will protect personal data against unauthorised or unlawful access, alteration, processing, disclosure, loss, destruction or damage. In particular:

• paper records containing personal data will be stored securely and not left unattended in areas accessible to others;

• confidential records will be locked away when not in use;

• portable devices and removable media containing personal data will be encrypted where possible and kept secure;

• personal data taken off site must be authorised, minimised, transported securely and returned or securely disposed of as soon as possible;

• staff must use strong passwords or passphrases and must not reuse school passwords for personal accounts;

• multi-factor authentication must be used where available;

• passwords must not be shared or written down where they can be accessed by others;

• staff must immediately report suspected phishing, malware, account compromise, unauthorised access or loss of equipment;

• staff must not store school personal data on personal devices unless specifically authorised and subject to appropriate safeguards;

• emails containing personal data must be checked carefully before sending and encrypted or otherwise protected where appropriate;

• access to Arbor, CPOMS and other systems will be restricted according to role and reviewed as needed.

The school maintains a records retention schedule covering pupil records, safeguarding files, SEND records, attendance, behaviour, admissions, complaints, exclusions/suspensions, staff files, recruitment, safer recruitment checks, accident records, examination records, finance and governance records.

15. Disposal of records

Personal data that is no longer required will be securely disposed of, deleted, anonymised or archived in line with the school's records retention schedule. Personal data that has become inaccurate or out of date will also be corrected or securely disposed of where appropriate.

Paper records will be shredded, placed in confidential waste or otherwise securely destroyed. Electronic records will be securely deleted, overwritten or removed from systems where possible. Where a third party is used for secure disposal, the school will ensure appropriate data protection and confidentiality arrangements are in place.

16. Personal data breaches

The school will take reasonable steps to prevent personal data breaches. All staff must report actual or suspected breaches to the DPO immediately and no later than the same working day.

A personal data breach may include, but is not limited to:

• emailing personal data to the wrong recipient;

• losing paper records, laptops, phones, USB drives or other devices containing personal data;

• unauthorised access to Arbor, CPOMS, email or shared drives;

• accidental publication of identifiable pupil or staff information;

• loss or inappropriate disclosure of safeguarding information;

• cyber attack, malware, phishing or account compromise;

• theft of equipment or records;

• inappropriate sharing with a third party.

The DPO will assess each breach and decide whether it must be reported to the ICO within 72 hours of the school becoming aware of it. Where a breach is likely to result in

a high risk to individuals' rights and freedoms, affected individuals will also be informed without undue delay unless an exemption or other lawful reason applies.

All breaches and near misses will be recorded in a breach log, including the facts, effects, decisions, actions taken and lessons learned. Significant breaches will be reported to the Proprietor. Safeguarding-related breaches will also be reviewed by the DSL or deputy DSL unless there is a conflict of interest, in which case alternative senior oversight will be arranged.

The school's breach procedure is set out in Appendix 1.

17. Training

All staff will receive data protection information and training as part of induction. Data protection will also form part of continuing professional development where changes to legislation, guidance, systems, risks or school processes make this necessary.

Training will cover confidentiality, appropriate use of school systems, safeguarding information sharing, recognising and reporting breaches, secure communication, password security, phishing risks, records retention and data subject rights. The school will keep a record of training attendance.

18. Monitoring arrangements

The Proprietor will monitor the operation of this policy and associated procedures. The DPO will support compliance monitoring, including review of breaches, SARs, DPIAs, privacy notices, processor arrangements and staff training.

This policy will be reviewed annually by the Proprietor, DPO and key staff, or sooner if there are significant changes to legislation, statutory guidance, ICO guidance, school systems, school structure or data protection risks.

Appendix 1: Personal data breach procedure

This procedure is based on ICO guidance on personal data breaches and applies to all staff, contractors and data processors working for or on behalf of the school.

1. On finding, causing or suspecting a personal data breach, the staff member or processor must immediately notify the DPO by emailing luke@new-direction.org.uk or by using the fastest available direct contact method. This must happen immediately and no later than the same working day.

2. The staff member must preserve evidence and take immediate safe steps to reduce risk, such as recalling an email, recovering documents, changing a password, disconnecting a compromised device or notifying a senior leader, where appropriate.

3. The DPO will investigate the report and determine whether a personal data breach has occurred. The DPO will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed, accessed or made available to unauthorised people.

4. Staff must co-operate with the investigation, including by providing information, devices, emails, records or explanations where required. The investigation will not automatically be treated as a disciplinary investigation, but disciplinary action may be considered where policies have been breached.

5. If a breach has occurred, or is likely to have occurred, the DPO will alert the Head of Education and, where significant, the Proprietor. Where the DPO has a conflict of interest, the Proprietor will arrange independent oversight or advice.

6. The DPO will make reasonable efforts to contain and minimise the impact of the breach. Relevant staff, IT providers, processors, insurers, safeguarding leads or professional advisers may be involved where necessary.

7. The DPO will assess the likely risk to individuals, considering the nature, sensitivity and volume of data, the number of people affected, the possible consequences, the likelihood of harm, the vulnerability of individuals and the steps already taken to mitigate risk.

8. The DPO will decide whether the breach must be reported to the ICO. Where reporting is required, this will be done without undue delay and, where feasible, within 72 hours of the school becoming aware of the breach.

9. Where the breach is likely to result in a high risk to individuals' rights and freedoms, the DPO will arrange for affected individuals to be informed without undue delay, unless an exemption or other lawful reason applies.

10. The DPO will document all breaches and near misses, whether or not they are reported to the ICO. The record will include the facts, cause, data involved, people affected, risk assessment, decisions, notifications, actions taken and lessons learned.

11. The DPO and relevant senior leaders will review the breach to identify learning, further training, technical improvements, procedural changes or disciplinary matters. Trends will be reviewed at least termly.

Actions to minimise the impact of specific breaches

Sensitive information disclosed by email, including safeguarding records

• The sender must attempt to recall the email immediately and notify the DPO.

• The DPO or IT provider will attempt technical recall or containment where possible.

• The recipient will be contacted and asked to delete the information, not to share, publish, save or copy it, and to confirm deletion in writing.

• The DPO will assess whether the breach must be reported to the ICO and/or affected individuals.

• Safeguarding-related breaches will be considered with the DSL or deputy DSL unless there is a conflict of interest.

Lost or stolen device or records

• The loss must be reported to the DPO immediately.

• The DPO will establish what data was involved, whether the device was encrypted, whether remote wipe is available and whether accounts or passwords need to be disabled.

• The police, insurer, IT provider, ICO and affected individuals will be notified where appropriate.

Cyber incident, phishing or account compromise

• The staff member must report the concern immediately and must not delete evidence.

• The school will involve IT support to secure accounts, reset passwords, revoke sessions, check forwarding rules, scan systems and assess unauthorised access.

• The DPO will assess whether personal data was accessed, altered, lost or disclosed and whether ICO or individual notification is required.

Accidental publication of personal data

• The information must be removed or access restricted as quickly as possible.

• The DPO will assess whether the data has been accessed, indexed, downloaded or further shared.

• The DPO will record the incident and determine whether reporting or individual notification is required.