



Every Child Matters Academy Trust
Children at the heart

GENERAL DATA PROTECTION REGULATION (GDPR) & INFORMATION SHARING POLICY 2026–2027

Written by:	Mrs. G. Foster-Wilson
Approved by:	Mr. W. Ward
Last reviewed:	October 2026
Next review due by:	October 2027

Contents

This policy sets out the Trust's framework for protecting personal information, using and sharing information lawfully, and meeting its safeguarding responsibilities.

1. Purpose, Scope & Accountability	3
2. Legal & Regulatory Framework	5
3. Data Protection Principles	6
4. Lawful Processing & Sensitive Information	7
5. Information Sharing & the New Statutory Duty	8
6. Security, Retention, Breaches & Individual Rights	11
7. Information Published on Websites	14
8. Suppliers, Data Processors & International Transfers	17
9. Freedom of Information & Other Disclosures	19
10. Training, Monitoring & Review	20
Appendix A – Information Sharing Decision Guide	22
Appendix B – Website Publishing Checklist	23
Appendix C – Privacy notice for pupils	24
Appendix D – Privacy notice for school workforce	28
Appendix E – Responding to subject access requests	31
Appendix F – Subject access request form	33
Appendix G & H – Confidentiality & data protection agreement 1 & 2	35
Appendix I & J – CCTV Signage advice & Operational checklist	37
Appendix K – Photo/Video/Artwork sharing consent	39
Appendix L – Parents who wish to photograph /video school events	40
Appendix M – Data collection form	41
Appendix N & O – Audit outline & Return	42
Appendix P – Data retention guidance	48
Appendix Q – Data sharing approval & assurance record	52
Appendix R – Disposal log	53

1. Purpose, Scope & Accountability

Purpose

Every Child Matters Academy Trust (“the Trust”) is committed to protecting personal information and using it fairly, lawfully, securely and transparently. The Trust recognises that effective information use and sharing are essential to education, administration, early help, safeguarding and the promotion of children’s welfare.

This policy explains how the Trust will meet its responsibilities under data protection law and how staff should handle information, including when information is shared with other organisations or published online.

Scope

This policy applies to all Trust academies, central Trust functions, governors, trustees, employees, volunteers, agency workers, contractors and other individuals who access or process information on the Trust’s behalf.

- It applies to information in electronic, paper, photographic, audio, video and verbal form where that information is personal data or confidential information.
- It applies to information held on Trust systems, school systems, cloud services, learning platforms, mobile devices, websites, social media and other approved systems.
- It applies when information is collected, created, accessed, used, analysed, shared, transferred, published, retained or destroyed.

Accountability and key roles

Trust Board and senior leadership

- The Trust Board has overall responsibility for ensuring compliance with data protection legislation and this policy, with appropriate governance and oversight arrangements in place.
- Provide effective governance and oversight of data protection and information security.
- Ensure sufficient resources, systems, training and controls are in place.

Data Protection Officer

- Coordinate data protection activities, including training and appropriate user-group or information-governance meetings.
- Maintain and update their own knowledge of developments in data protection and information governance.
- Undertake or coordinate systematic data protection compliance audits and maintain records of incidents, remedial actions and recommendations

- Assist with investigations into complaints or breaches and undertake or coordinate reporting and remedial action as required.
- Maintain and coordinate records of subject access requests and other formal data protection rights requests.
- Provide expert advice and act as a resource for staff on data protection and related information-governance issues.
- Provide independent advice, monitoring and support on data protection compliance and information governance.
- Advise on DPIAs, data sharing, privacy notices, data protection rights, incidents and high-risk processing.
- Act as the appropriate contact for the ICO where required and support the management of data protection complaints.

Designated Safeguarding Lead and safeguarding staff

Headteachers:

- Each Headteacher is responsible for the successful implementation of this policy within their school and for ensuring that appropriate local arrangements are in place.
- The Headteacher will authorise the release of information in connection with a subject access request where this is required under the Trust's procedures and will ensure that secure arrangements are in place for sensitive records.
- Ensure information sharing supports the Trust's child-centred safeguarding responsibilities and follows local safeguarding pathways.
- Escalate safeguarding information promptly where a child may need help, support or protection.

All staff and other users of Trust information

- All staff and contractors who collect, access or process personal data are responsible for complying with this policy and for keeping personal information secure and confidential.
- Staff must ensure that personal information they provide to the Trust in connection with their employment is accurate and up to date and must notify the Trust promptly of changes to their own personal information, such as a change of address.
- Staff must report any unauthorised disclosure, loss of personal data or other suspected breach immediately to the DPO and must not delay reporting while investigating the incident themselves.
- Only access information needed for legitimate duties and responsibilities.
- Keep information secure, accurate and confidential, and report suspected breaches or inappropriate disclosure immediately.
- Share relevant safeguarding information when the law and this policy require or permit it; staff must not allow uncertainty about data protection to become a barrier to safeguarding.

Remember

Data protection law is not a barrier to appropriate safeguarding information sharing. It provides a framework for sharing information lawfully, fairly, proportionately and securely.

2. Legal & Regulatory Framework

The Trust will comply with applicable UK legislation and have regard to relevant statutory guidance and regulatory guidance. This policy is written for England and is reviewed to reflect changes in law and guidance.

Key legislation

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018 (DPA 2018).
- Data (Use and Access) Act 2025 (DUAA), including changes that came into force in 2026.
- Children Act 2004, including section 16LA as amended by the Children's Wellbeing and Schools Act, establishing the information sharing duty from 30 September 2026.
- Privacy and Electronic Communications Regulations 2003 (PECR), including rules on cookies and similar technologies and electronic communications.
- Freedom of Information Act 2000 and associated information access requirements, where applicable to the Trust.
- Equality Act 2010, including duties relevant to accessibility and non-discriminatory processing.
- Copyright, Designs and Patents Act 1988 and other intellectual property law where information, images or creative work are published or shared.

Key statutory guidance and regulatory guidance

- Keeping Children Safe in Education 2026 (KCSIE), including its requirements concerning information sharing, record keeping and online safety.
- Working Together to Safeguard Children 2026.
- Information Sharing Duty: Statutory Guidance for safeguarding organisations and their practitioners, September 2026.
- Department for Education guidance on data protection in schools and privacy notices, updated in 2026.
- Information Commissioner's Office (ICO) Data sharing Code of Practice and guidance on children's information, lawful bases, security, DPIAs, transparency, cookies and individual rights.

Related Trust policies and procedures

- Safeguarding Policy and procedures.
- Data Breach / Security Incident Management procedures and ICT Disaster Recovery Procedure and Plan
- ICT Security and Usage Policy and Staff Acceptable Use Policy
- ICT Cyber Awareness Plan
- AI Policy
- Records Management, Freedom of Information and Subject Access Request procedures.

Important

Where a local safeguarding procedure, data sharing agreement or statutory pathway sets out a specific route for sharing information, staff should use that route. A data sharing agreement is helpful but the absence of an agreement must not prevent lawful safeguarding information sharing where the statutory criteria are met.

3. Data Protection Principles

The Trust will apply the data protection principles whenever it processes personal data. Staff must be able to demonstrate that their processing is lawful and appropriate.

Lawfulness, fairness and transparency

Information must be processed lawfully, fairly and transparently. People should understand how their information is used, subject to lawful exceptions where providing information would undermine safeguarding or another legal purpose.

Purpose limitation

Information must be collected for specified, explicit and legitimate purposes and not used in ways incompatible with those purposes.

Data minimisation

Only information that is adequate, relevant and necessary for the purpose should be collected, accessed or shared.

Accuracy

Reasonable steps must be taken to ensure information is accurate and, where necessary, kept up to date. Opinions, professional judgements and allegations should be clearly distinguished from established facts.

Storage limitation

Personal information must not be kept longer than necessary and must be disposed of securely.

Integrity and confidentiality

Appropriate technical and organisational measures must protect information against unauthorised or unlawful processing, accidental loss, destruction or damage.

Accountability

The Trust must be able to demonstrate compliance through policies, records, training, DPIAs, contracts, audits and documented decision-making.

Data protection by design and default

Privacy and security must be considered at the start of new projects, systems, websites, data collections and information-sharing arrangements. The Trust will use proportionate privacy-by-design measures and will complete a Data Protection Impact Assessment (DPIA) where required or where processing is likely to create a high risk to individuals.

Particular care is required when processing children's information. The Trust will consider children's best interests, age, understanding, vulnerability and reasonable expectations when designing services and using their information.

4. Lawful Processing & Sensitive Information

Lawful basis

Before collecting, using or sharing personal data, the Trust must consider;

- Consent – where a clear, specific, informed and freely given choice is appropriate.
- Contract – where necessary to perform or enter into a contract.
- Legal obligation – where the Trust is required by law to process the information.
- Vital interests – where necessary to protect someone's life in limited circumstances.
- Public task – where processing is necessary for the Trust's public functions or tasks in the public interest, where applicable.
- Legitimate interests – where permitted and where the required balancing test has been completed.
- Recognised legitimate interests – where the statutory conditions introduced through the Data (Use and Access) Act 2025 apply.

The appropriate lawful basis will depend on the particular processing activity. Staff should seek advice from the DPO where the basis is unclear.

Special category data

Special category information includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health, sex life or sexual orientation. Processing also requires an additional Article 9 condition, and in some cases a DPA 2018 Schedule 1 condition and appropriate policy documentation.

Criminal offence information

Information about criminal convictions, offences and related allegations is subject to additional legal requirements. Staff must not share such information routinely or informally. The DPO should be consulted where the lawful authority or condition is unclear.

Children and young people

Children have data protection rights and should receive privacy information that is clear, accessible and appropriate to their age and understanding. The Trust will use child-friendly explanations where appropriate and will consider the child's best interests when processing or sharing information.

Automated decision-making and profiling

The Trust will identify and control any processing involving automated decision-making or profiling that has legal or similarly significant effects. Such processing must be assessed for lawfulness, fairness, transparency, accuracy, bias and appropriate human oversight before use.

Consent is not a universal solution

For safeguarding and welfare information sharing, consent is often not the appropriate lawful basis. The statutory information sharing guidance makes clear that legal obligation, public task or another appropriate lawful basis may apply. Staff must not create a false choice by asking for consent where information will be shared regardless.

5. Information Sharing & the New Statutory Duty

Effective information sharing is essential to identifying need early, safeguarding children, preventing escalation and coordinating support. From 30 September 2026, the information sharing duty under section 16LA of the Children Act 2004, as amended by the Children's Wellbeing and Schools Act, provides a clear statutory duty for organisations within its scope.

When the duty applies

The duty applies where a relevant organisation or practitioner holds information about a child, or another individual connected to a child, and considers that the information is relevant to safeguarding or promoting the welfare of the child. It applies to children with known needs and children whose needs are being identified for the first time.

- There is no requirement to wait until a child meets a particular statutory threshold before relevant information can be shared under the duty.
- Relevant information may support assessment of need or risk, decision-making, provision of support, or action to safeguard and promote welfare.
- The duty can apply where information relates to a child who may pose a risk to others, where the information is relevant to safeguarding and promoting welfare.
- The duty may apply to information about another named individual connected to the child where that information is relevant to the child's welfare.

The statutory duty also applies when a relevant organisation or practitioner requests information from another relevant organisation or practitioner. Requests should be considered promptly against the statutory criteria, and information should be shared where the criteria are met, subject only to the very limited detriment exception.

The duty to share

Where the statutory criteria are met, information must be shared with another relevant organisation or practitioner where the person holding the information considers that sharing may facilitate the recipient's relevant safeguarding or welfare functions.

The very limited detriment exception

When considering whether sharing could be more detrimental to the child than not sharing, practitioners should consider whether the risk can be reduced by limiting the information shared, using a safer sharing route or removing unnecessary identifying details. Where only part of the information creates a risk, the relevant safeguarding information should still be shared where possible. If the decision is finely balanced, staff should seek prompt advice from the DSL, safeguarding lead, manager or other appropriate professional adviser, including the DPO where data protection questions arise.

The duty does not apply where the practitioner, using professional judgement on behalf of the organisation, determines that disclosure would be more detrimental to the child than not disclosing it. This exception is expected to be rare. The decision must be carefully considered, focused on the child's welfare, documented and reviewed.

The decision-making tests

Relevance - Does the information have a bearing on safeguarding or promoting the child's welfare?

May facilitate - Could sharing reasonably help the recipient assess need or risk, make a decision, provide support or take safeguarding action?

Detriment - Could sharing cause greater detriment to the child than not sharing? Can the risk be mitigated by limiting the information or using a safer route?

Proportionality - What is the minimum information necessary for the recipient to fulfil the relevant function?

Consent and transparency

Staff must distinguish between consent as a data protection lawful basis, consent to receive a service, and consent relating to confidentiality. None of these should be treated as a requirement to obtain permission before sharing where the statutory information sharing duty applies. Staff should also consider any applicable common law duty of confidentiality and relevant professional standards. A parent or child objecting to sharing, fear of criticism or complaint, or practitioner uncertainty does not by itself prevent lawful information sharing where the statutory criteria are met.

Consent is not required to share information under the information sharing duty. The Trust will normally be open and transparent with children and families about what information is shared, with whom and why, unless doing so would increase risk, undermine safeguarding, or is otherwise not safe or practicable. Where information must be shared under a legal obligation, staff should not present sharing as optional.

Confidentiality

The statutory guidance confirms that the information sharing duty supports lawful disclosure of confidential information where its criteria are met and data protection requirements are satisfied. Staff must still share only information that is relevant, necessary and proportionate and must use secure routes.

Sharing across organisations and geographical boundaries

Where a child is moving between schools, areas or services, the Trust will proactively share relevant safeguarding and welfare information through appropriate routes so that important information is not lost. A formal data sharing agreement is not a precondition to sharing where the statutory criteria are met.

Recording decisions

Information-sharing decisions should be kept under review as further information is received or the level of risk and need changes. Where information is not shared, the record should explain what was withheld and why. Where appropriate, staff should seek further information from other organisations to improve the assessment of need and risk. Decisions and rationales for routine or strategic information-sharing arrangements should be documented and reviewed regularly.

Staff must be able to demonstrate accountability. Where appropriate, records should show what information was shared or withheld.

Local safeguarding arrangements

The Trust will work in accordance with published local safeguarding arrangements and agreed information-sharing protocols. Where multi-agency arrangements or data sharing agreements apply, these should make clear what information is shared, between which organisations or practitioners, at what point and through which mechanism. Different routes may be appropriate for formal referrals, early help or Family Help, routine information and urgent safeguarding information. Staff must know the agreed local routes and who to contact when information needs to be shared with another area or service.

Where local safeguarding partners have agreed that particular information is necessary to identify need, risk or emerging harm, information may be shared regularly rather than only following an individual incident or referral. Examples may include school attendance or patterns of absence, including information relevant to the risk of becoming NEET, where this has been identified locally as relevant. Any such arrangement must comply with data protection law and should support timely, joined-up responses and early intervention.

Staff must use the local safeguarding partnership's agreed pathways, referral routes and secure systems. The DSL will ensure that staff know how to make urgent referrals and how to share information where a child may be at immediate risk.

6. Security, Retention, Breaches & Individual Rights

Information security

- Use Trust-approved systems and accounts for Trust information.
- Use strong passwords, multi-factor authentication and access controls where provided.
- Do not leave personal information visible, unattended or accessible to people without a legitimate need to know.
- Check email recipients and attachments before sending personal information, especially sensitive information.
- Use secure transfer mechanisms approved by the Trust when sharing information externally.
- Do not use personal email accounts, unapproved cloud storage, consumer messaging services or removable media for Trust personal data unless specifically authorised.

- Lock devices when unattended and report lost or stolen equipment immediately.

Data quality and records

CCTV arrangements:

- Where CCTV is used at a Trust school, it is used to support the prevention and detection of crime and other identified safety or operational purposes. Its use must be reflected in the relevant school privacy information.
- Staff, parents, pupils and visitors must be informed that CCTV is in operation through appropriate signage displayed at key points around the site. Signage should make clear that CCTV is in use and identify the responsible organisation or appropriate contact arrangements.
- Access to CCTV footage must be restricted to designated authorised staff, or designated employees of an approved PFI/provider arrangement where applicable. Footage must not be viewed, copied or disclosed by unauthorised persons.
- CCTV recordings must be retained only for the period necessary for the stated purpose and then securely deleted or overwritten. Any disclosure of footage must be lawful, necessary and appropriately recorded.
- Schools operating CCTV must maintain appropriate operational arrangements and review compliance with the Trust's data protection and CCTV requirements regularly.

Records should be factual, relevant, proportionate and contemporaneous. Where professional judgement is recorded, it should be identified as opinion and supported by the information available at the time. Records should be written with the possibility that they may be disclosed to the data subject or another lawful recipient.

Retention and disposal

- The Trust will operate a Records Retention Schedule to determine how long documents containing personal data should be retained, in line with applicable statutory, regulatory and professional requirements.
 - When records are no longer required or the applicable retention period has been met, paper records containing personal data must be securely shredded or incinerated. Where disposal is commissioned to a third party, appropriate records of destruction must be maintained.
 - Electronic devices containing personal data must be securely formatted and destroyed by an approved contractor, with a certificate of destruction obtained for each disposal where applicable.
- Personal data will be retained only for as long as necessary under applicable statutory or professional requirements. Records must be securely deleted, destroyed or anonymised when the retention period expires, subject to lawful holds or ongoing investigations.

Personal data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending information to the wrong person, losing a device, publishing confidential information online or giving inappropriate access to a system.

All suspected breaches must be reported immediately through the Trust's data breach procedure. Staff must not delay reporting while trying to establish whether a breach is technically reportable. The DPO will assess the incident, containment, notification and regulatory reporting requirements.

The Trust will assess each breach on a case-by-case basis. The ICO must be notified where the breach is likely to result in a risk to the rights and freedoms of individuals. Examples of potential significant harm include discrimination, damage to reputation, financial loss, loss of confidentiality or other significant social disadvantage.

The threshold for notifying affected individuals is higher. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust must notify the individuals concerned directly without undue delay, subject to any applicable legal exception.

A breach notification to the ICO should include, where available: the nature of the breach; the categories and approximate number of individuals concerned; the categories and approximate number of personal data records concerned; the name and contact details of the DPO; the likely consequences of the breach; and the measures taken or proposed to address the breach and mitigate adverse effects.

Where notification to the ICO is required, it must be made without undue delay and, where feasible, within 72 hours of the Trust becoming aware of the breach. If all information is not available within that period, information may be provided in phases.

Staff must inform the DPO immediately of any suspected personal data breach so that investigation, containment and any required notification process can begin. Failure to report a breach promptly may be managed under the Trust's relevant staff procedures.

Individual data protection rights

- Right to be informed – individuals should be given clear information about how their personal data is collected and used, including relevant purposes, lawful bases, sharing, retention and their rights, subject to lawful exceptions.
- Right of access – individuals can request access to personal information held about them, subject to the applicable legal requirements and exemptions. Requests must be managed through the Trust's established subject access request procedure.
- Right to rectification – individuals can ask for inaccurate or incomplete personal data to be corrected. Where appropriate and possible, the Trust should inform relevant third parties to whom the inaccurate data has been disclosed of the rectification.

- Right to rectification – individuals can ask for inaccurate or incomplete personal data to be corrected. Where appropriate and possible, the Trust should inform relevant third parties to whom the inaccurate data has been disclosed of the rectification.
- Right to erasure – in certain circumstances, individuals can request the deletion or removal of personal data where there is no compelling lawful reason for its continued processing. This right is not absolute and does not apply where the law requires or permits continued retention.
- Right to restrict processing – in certain circumstances, individuals can require the Trust to restrict the use of their personal data. While processing is restricted, the Trust may retain the information but should not otherwise process it except where the law permits.
- Right to data portability – where the legal conditions apply, individuals can obtain and reuse their personal data for their own purposes across different services and may ask for it to be transferred in a structured, commonly used and machine-readable format.
- Right to object – individuals may have the right to object to particular processing depending on the lawful basis and circumstances. The Trust will consider and respond to objections in accordance with the law.
- Rights relating to automated decision-making and profiling – where these rights apply, individuals will be provided with the protections required by data protection law, including appropriate human involvement and routes to challenge decisions where applicable.

Requests should be passed promptly to the Trust's DPO or the designated subject access request process. Staff must not respond independently to a formal rights request unless authorised to do so.

Requests from parents and carers

Parents and carers do not automatically have a right to access all information held about a child. The Trust will consider the child's age, understanding, wishes, the nature of the information, parental responsibility and any safeguarding concerns when responding to requests involving a child's personal data.

7. Information Published on Websites

The Trust recognises that information published on a school or Trust website may be accessible to a very large audience and may be copied, downloaded, indexed by search engines or shared through social media. Website publication must therefore be treated as a disclosure of information and checked before publication.

Privacy notices and transparency

- The Trust and academies will make relevant privacy notices freely available and accessible through their websites.
- Privacy notices must explain what personal data is processed, why it is processed, the lawful basis, relevant sharing, retention, rights and contact details, and should reflect significant changes in processing.
- Privacy information should be written clearly and, where children are the audience, in age-appropriate language or with child-friendly explanations.
- Website privacy notices should be reviewed at least annually and whenever there is a significant change to processing.

Publishing pupil information

- Do not publish personal information about a pupil unless the publication is necessary, proportionate and consistent with the Trust's privacy information and safeguarding arrangements.
- Avoid publishing unnecessary combinations of information that make a child identifiable, particularly where the child may be vulnerable or at increased risk.
- Never publish information that could disclose a child's confidential address, location, care arrangements, medical information, safeguarding status or other sensitive details unless there is a specific lawful basis and it is safe and necessary to do so.
- Particular care must be taken with children subject to court orders, safeguarding restrictions, witness protection arrangements or other confidentiality measures.

Photographs and videos

Identifiable photographs and videos are personal data when used for official school purposes. Before publication, staff must check the Trust's current permissions, lawful basis and any safeguarding restrictions. Images must be appropriate, relevant to the stated purpose and published at an appropriate level of detail.

Where consent is the lawful basis, it must be valid and capable of being withdrawn. Where another lawful basis is relied upon, the Trust will still consider whether families have been given appropriate information and an opportunity to raise concerns or opt out where the Trust's procedures provide for this.

Specific photography and video arrangements:

- The Trust may use photographs and digital images, including video, for purposes such as capturing development and progress in learning; school prospectuses and other publications promoting the school or Trust; assemblies and celebration events; sports day; school performances; and trips and residential outings.

- Where images of children or staff are used in public areas or made available online, including through the school website or social media, staff must check the applicable lawful basis and the Trust's photography consent arrangements before publication. The relevant consent form and parent/carers guidance are retained at Appendix K and Appendix L of this policy.
- Consent arrangements must distinguish, where applicable, between different uses of images, such as website publication, school displays and class projects, social media, media publication and school photographs. Staff must not assume that consent for one purpose automatically authorises another purpose.
- For school events, the Headteacher is responsible for deciding whether photography or videoing is permitted and the conditions that apply, including arrangements intended to safeguard children and minimise disruption. Parents and carers using cameras or video at school events must follow the school's instructions and any restrictions communicated by staff.

Pupil work, names and achievements

Pupil work may contain personal data and intellectual property. Before publishing work, names, awards, competition results or other achievements, the Trust must check the relevant privacy arrangements, permissions and safeguarding considerations. Where possible, publication should minimise unnecessary identifying information.

Staff and governor information

Only information that is necessary and appropriate for a professional or statutory purpose should be published. Personal home addresses, private telephone numbers, personal email addresses, dates of birth and other unnecessary personal details must not be published.

Website forms and enquiries

Online forms must collect only information necessary for the stated purpose. Forms collecting personal or sensitive information must use appropriate security, provide privacy information at the point of collection where appropriate, and route submissions to authorised staff. Sensitive safeguarding information should not normally be requested through a general website contact form.

Cookies and similar technologies

Websites must comply with PECR and data protection law when using cookies, tracking pixels, local storage, scripts, tags or other technologies that store or access information on a user's device. Non-essential technologies generally require prior consent that meets the UK GDPR standard, unless a specific legal exception applies.

- The Trust will maintain an inventory of cookies and similar technologies used on its websites.
- Users will be given clear information about what technologies are used and why.
- Non-essential analytics or tracking technologies will not be activated before valid consent where consent is required.

- Third-party services and embedded content will be assessed for data protection, security, international transfer and tracking implications.

Accessibility and online documents

Website content and documents must be accessible. New documents should be created with appropriate headings, readable fonts, meaningful link text, alternative text where needed and accessible document structure.

Website governance

- Website editors must receive appropriate training and know who to contact for data protection and safeguarding advice.
- Content owners should regularly review published information and remove or amend information that is inaccurate, outdated, excessive or no longer required.
- A process should exist for rapidly removing or correcting information where publication creates a safeguarding, privacy or security concern.
- Websites should not be used to publish internal case information, complaint correspondence, staff disciplinary information or other confidential records.

Website rule

If information would be inappropriate to put on a public noticeboard outside the school, it is unlikely to be appropriate to publish it on the website. Public visibility should be treated as a significant disclosure.

8. Suppliers, Data Processors & International Transfers

Due diligence before procurement

Before introducing a new system, platform, app or service that processes personal data, the Trust will assess its privacy, security, safeguarding, functionality and contractual risks. A DPIA will be completed where required or appropriate.

- Identify what personal data will be processed and why.
- Identify whether special category, criminal offence or children's data will be processed.
- Check supplier security, retention, deletion, access and incident arrangements.
- Confirm whether the supplier acts as a processor or independent controller and document the relationship.
- Check international transfers and the safeguards relied upon.
- Check whether data will be used for analytics, profiling, advertising, AI model training or other secondary purposes.

Data processing agreements

Where a supplier processes personal data on the Trust's behalf, the Trust will have an appropriate written contract or data processing agreement containing the required data protection provisions. Suppliers must only process data in accordance with documented instructions and must provide appropriate security and assistance with data protection obligations.

International transfers

Personal data must not be transferred outside the UK, or made accessible from another country, without appropriate assessment and safeguards. The Trust will follow current ICO requirements for international transfers and document the mechanism relied upon.

Data sharing agreements

Where the Trust participates in a multi-agency safeguarding partnership, the partnership should have a data sharing agreement alongside its published local arrangements. The agreement should be reviewed and updated to reflect the statutory information sharing duty and should provide clarity about what, when and how information is shared. An overarching Data Protection Impact Assessment is likely to be required before a partnership agrees a new data sharing arrangement where the proposed processing creates risks that need to be assessed.

- Trust schools may use external agencies to provide one-to-one guidance and support services to pupils, including Educational Psychology, Speech and Language Therapy (SALT) and counselling services. Where these services operate on school premises, the data protection and confidentiality arrangements must be agreed in advance.
- Many such services operate confidentially and may only share information with the school or parents with the pupil's consent where appropriate, or where an overriding duty of care or safeguarding concern requires disclosure. The precise arrangements must reflect the service being provided and applicable law.
- The school must decide at the outset whether the service will operate under its own agreed confidential arrangements or within the school's information-handling requirements. This must be communicated clearly to pupils and parents/carers to avoid incorrect assumptions about confidentiality.
- The school's expectations about confidentiality, information sharing, access to records and safeguarding disclosures must be clearly stated in the Service Level Agreement (SLA) or other written agreement with the external agency. The SLA should require agency staff to explain the confidential nature, or limits of confidentiality, of the service to pupils and parents/carers.

Data sharing agreements are recommended where organisations routinely exchange personal information. They should clarify purpose, lawful basis, categories of data, roles, security, retention, access, onward sharing, incident management and review arrangements. However, staff must not treat the absence of a formal agreement as a reason to delay a lawful safeguarding disclosure.

9. Freedom of Information & Other Disclosures

Freedom of Information

The Trust will comply with the Freedom of Information Act 2000 and its related duties. Requests for recorded information should be passed promptly to the person responsible for FOI handling. Staff must not disclose information informally simply because a request has been made.

Subject access and other statutory requests

Formal requests for personal data or other information will be managed through the Trust's established procedures. Staff must preserve relevant records and must not delete or alter information in response to a request unless authorised under normal records management arrangements.

Law enforcement and other statutory disclosures

The statutory information sharing duty does not cover every possible recipient. Where information needs to be shared with organisations such as charities, private healthcare providers, community-based organisations or other professionals outside the scope of the duty, staff must consider the alternative legal power or duty that permits the sharing and any applicable common law duty of confidentiality. The Trust should consider whether the sharing is necessary, relevant and proportionate, and whether the recipient has appropriate security arrangements. Organisations outside the duty should be encouraged to provide relevant information to statutory safeguarding partners where this supports the safety and welfare of children.

- Personal data may be disclosed to third parties where a lawful basis or statutory route permits or requires disclosure. Examples include publishing examination results or other pupil achievements; sharing relevant medical information where necessary in the pupil's interests, such as for medical advice, insurance purposes or school trips; transferring information to another educational establishment; providing information to examination authorities; and making statutory returns or disclosures to government departments such as the Department for Education or to Ofsted.
- Other lawful disclosures may include sharing information for the prevention or detection of crime, to prevent serious harm to the data subject or another person, for tax or other legal purposes, for legal proceedings or to obtain legal advice. Only information that is necessary and proportionate should be disclosed.
- When a request for personal data is received from a third party, reasonable steps must be taken to verify the identity of the requester and establish why the information is required. Where consent is required and has not been given, and no lawful exception applies, the request must be declined.

- Personal information should not normally be disclosed to third parties over the telephone. In most circumstances, the requester should provide documentary evidence to support the request, such as evidence of identity, authority or the legal/statutory basis for the request.
- When providing information to an individual, including by telephone, the recipient's identity must be verified. Staff must take particular care not to disclose information to another person merely because they are related to the individual concerned.

Information may need to be disclosed to the police, local authority, courts, safeguarding partners, regulators, professional bodies or other statutory organisations. Staff must identify the relevant legal basis, authority or statutory route and disclose only information that is necessary and proportionate, unless a specific legal requirement dictates otherwise.

Emergency disclosures

In an emergency, information may need to be shared rapidly to protect a child or another person from serious harm. Data protection law allows proportionate emergency sharing where the appropriate lawful basis and safeguards apply. Staff should use the safest available route and record the decision as soon as practicable afterwards.

External publication and media enquiries

- Concerns about the Trust's handling of personal data should normally be raised with the Trust first. Where an individual remains concerned, or where the matter is appropriate for regulatory consideration, the Information Commissioner's Office (ICO) can be contacted at <https://ico.org.uk/concerns/> or by telephone on 0303 123 1113.
- The DPO should support the Trust in responding to information-handling complaints and regulatory correspondence where appropriate.

Media enquiries, requests for statements and requests to publish case-related information must be referred to the Trust's authorised communications lead. Staff must not confirm personal information or comment on individual children, families or staff without authority.

10. Training, Monitoring & Review

Training

- All staff who handle personal data will receive appropriate training.
- Training will cover confidentiality, data protection principles, information sharing, safeguarding, cyber security, breach reporting and the Trust's local procedures.
- Staff whose roles involve higher-risk processing will receive additional role-specific training.
- Website editors and staff responsible for publishing information will receive specific guidance on privacy, safeguarding, images, accessibility and online publication.

Monitoring and assurance

Where agreed information-sharing routes or mechanisms are not followed, the Trust will use appropriate feedback, incident-management and escalation arrangements to identify learning, improve processes and reduce the likelihood of recurrence. Information-sharing arrangements should be monitored and reviewed to ensure they remain proportionate, secure, effective and consistent with local safeguarding arrangements.

- The Trust will monitor compliance, such as through audits, incident trends, training records, rights requests, website checks and supplier assurance.
- Information sharing arrangements will be reviewed with local safeguarding partners and relevant organisations as appropriate.
- The DPO will report significant risks, incidents and compliance issues through the Trust's governance arrangements.

Breaches of this policy

Failure to follow this policy may expose individuals, children and the Trust to privacy, safeguarding, security and legal risks. Deliberate or serious breaches may be managed under relevant Trust procedures, including disciplinary procedures where appropriate.

Review

This policy will be reviewed at least annually and sooner where there are significant changes to legislation, statutory guidance, ICO guidance, Trust systems or information-sharing arrangements. The next scheduled review is October 2027.

Appendix A – Information Sharing Decision Guide

This checklist supports professional judgement. It does not replace the DSL, local safeguarding procedures, the statutory information sharing guidance or advice from the DPO / Information Governance Lead.

1. What information do I hold?

Identify the information, its source, its accuracy and whether it includes special category or criminal offence data.

2. Why might it be relevant?

Consider whether it may help safeguard or promote the welfare of a child, identify need, assess risk, make a decision or provide support.

3. Who needs it?

Identify the recipient and confirm their relevant safeguarding or welfare function. Use the agreed local pathway where one exists.

4. Does the information sharing duty apply?

If the statutory criteria are met, relevant information must be shared unless the very limited detriment exception applies.

5. What lawful basis applies?

For the statutory duty, legal obligation is likely to be relevant. Public task or another appropriate lawful basis may apply in other circumstances. Consider Article 9 / Schedule 1 requirements where necessary.

6. How much should I share?

Share information that is relevant, necessary and proportionate. Avoid unnecessary details.

7. Could sharing itself harm the child?

Consider whether disclosure would be more detrimental to the child than not sharing. If so, record the reasoning and seek advice.

8. Have I considered transparency?

Where safe and practicable, explain to the child and/or family what is being shared, with whom and why. Do not seek consent where it is not required or would create a false choice.

9. How will I share securely?

Use the agreed secure route and check the recipient before sending. Do not use personal email or unapproved systems.

10. Have I recorded the decision?

Record what was shared or not shared, why, with whom, the lawful basis, any risks considered and any follow-up action.

If in doubt

Safeguarding concerns should be discussed promptly with the DSL or Deputy DSL. Data protection advice should be obtained from the DPO. Do not delay urgent safeguarding action while waiting for routine administrative advice.

Appendix B – Website Publishing Checklist

- Is the information necessary and appropriate to publish publicly?
- Is there a documented lawful basis for any personal data?
- Have the Trust privacy notice and relevant privacy information been considered?
- Does the information identify a child, family member or staff member unnecessarily?
- Have safeguarding restrictions, court orders or confidentiality arrangements been checked?
- If using a photograph or video, have the applicable permissions, lawful basis and publication conditions been checked?
- Is pupil work being published with appropriate privacy and intellectual property considerations?
- Are staff contact details limited to professional information that is necessary?
- Does the page or form collect any personal data? If so, is the collection necessary, secure and transparent?
- Are cookies, analytics, tracking pixels, scripts or embedded third-party services being used? Have PECR and privacy requirements been checked?
- Is the content accurate and up to date?
- Is the page or document accessible, including headings, link text, images, PDFs and multimedia?
- Is there a clear owner responsible for reviewing and removing the information when no longer required?
- Could publication create a safeguarding, privacy, reputational or security risk? If yes, stop and seek advice before publishing.

Appendix C – Privacy notice for pupils

ECM Academy Trust is a data controller for the Purposes of the General Data protection Regulation 2018 and as such is registered with the Information Commissioners Officer. We collect information from you and may receive information about you from your previous school.

Why do we collect and use pupil information?

We collect and use pupil information under the Data Protection Act 1998 (DPA) and “Article 6” and “Article 9” of the General Data Protection Regulation (GDPR).

Article 6 (GDPR) condition: processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 9 (GDPR) condition: the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

We use the pupil data to:

- support pupil learning;
- monitor and report on pupil progress;
- provide appropriate pastoral care;
- assess the quality of our services;
- comply with the law regarding data sharing; and
- safeguard pupils.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- SEN information
- Exclusions/behavioural information

We may also receive information from their previous school or college, local authority and the Department for Education (DfE).

Note: Schools and local authorities have a (legal) duty under the DPA and the GDPR to ensure that any personal data they process is handled and stored securely

For details of what we collect, hold and share, please visit the Information Commissioner’s Office (ICO) Data Protection Register on <https://ico.org.uk/esdwebpages/search> and enter **Z9204596**.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to

us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data in line with our Records Management Policy. After which this is securely disposed of by only using accredited data disposal companies.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us;
- our local authority;
- the Department for Education (DfE);
- school nurse;
- EWO;
- Medical practitioners;and
- ECM Trust.

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Deb Barker on 01226 273220 or d.barker@ecmtrust.co.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance to:-

Mrs D Barker
Data Protection Officer
Every Child Matters Academy Trust
Newsome Avenue
Wombwell
Barnsley
S73 8QS

01226 273220

d.barker@ecmtrust.co.uk

or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Contact:

If you would like to discuss anything in this privacy notice, please contact:

Deb Barker on 01226 273220 or d.barker@ecmtrust.co.uk

Appendix D – Privacy Notice for school workforce

Every Child Matters Academy Trust is a data controller for the Purposes of the General Data Protection Regulation 2018 and as such is registered with the Information Commissioners Officer.

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body and the School Support Staff Negotiating Body

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, NI number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid

We collect and use pupil information under the Data Protection Act 1998 (DPA) and "Article 6" and "Article 9" of the General Data Protection Regulation (GDPR).

- *Article 6 (GDPR) condition:* processing is necessary for **compliance with a legal obligation** to which the controller is subject
- *Article 6 (GDPR) condition:* 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
- *Article 9 (GDPR) condition:* the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a

voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so,

- our local authority – we are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments
- The Department for Education (DfE) – We share personal data with the DfE on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation and links to school funding/expenditure and the assessment educational attainment. We are required to share information about our workforce members with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments
- HMRC for legal purposes

This data is stored for as long as is required under statutory requirements. Please see the school document retention policy for details of this. Any data is then disposed of using only accredited secure disposal companies.

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and

- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department: <https://www.gov.uk/contact-dfe>

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection Officer, Mrs D Barker on 01226 206788 or d.barker@ecmtrust.co.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

If you would like to discuss anything in this privacy notice, please contact:

Mrs D Barker on 01226 273220 or d.barker@ecmtrust.co.uk

Appendix E - Procedures for responding to subject access requests made under the GDPR 2018

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the GDPR 2018 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005 (Pupil Information Regulations).

These procedures relate to subject access requests made under the GDPR 2018.

Processing a subject access request

1. Requests must be made in writing; and be addressed to the Head teacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
 - passport
 - driving licence
 - utility bills with the current address
 - Birth / Marriage certificate
 - P45/P60
 - Credit Card or Mortgage statement

(This list is not exhaustive).

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.
4. The response time for subject access requests, once officially received, is 40 days (**not working or school days but calendar days, irrespective of school holiday periods**). However any disclosure of personal data will not take place until after clarification of information sought.
5. The GDPR 2018 allows exemptions as to the provision of some information; therefore all

information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information, consent will be obtained where this is required. The 40 day statutory timescale will still be adhered to.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another will not be disclosed, nor will information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice will be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed will be presented in a clear format, any codes or technical terms will be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it will be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail will be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Board of Trustees who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Mrs D Barker on 01226 273220 / d.barker@ecmtrust.co.uk

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113

Appendix F - Subject Access Request Form

Request for information under the GDPR 2018

This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type. (* Required Fields).

1. Personal details of the person requesting the information

Surname	
Forename	
Address	
Postcode	
Telephone Number	
Email Address	

2. Are you the Data Subject (i.e the person whose information you are requesting)?

Please tick the appropriate box

Yes

☐

No

☐

3. Personal Details of Data Subject (if different from those in section 1)

Surname	
Forename	
Address	
Postcode	
Telephone Number	
Email Address	
Date of Birth	
School Attended	

4. If you are not the Data Subject please describe your relationship with the Data Subject that leads you to make this request on their behalf

5. Information Requested

If you would like to see only specific documents please describe these below

6. If you would like a full copy of the personal records held by the school, please tick here ☐.

Declaration

I certify that the information given in this application form to the school is true. I understand that it will be necessary for the school to confirm my/the Data Subject's identity and it may be necessary to supply more detailed information if required.

Signature (Person requesting the information)

Print name

Date:

GDPR 2018

The Data Controller is Every Child Matters Academy Trust (The Trust)

The details you provide on this form will only be used in connection with your application for the supply of documents and for statistical purposes.

The completed form should be returned to:

Data Protection Officer
Every Child Matters Academy Trust
Newsome Avenue
Wombwell
Barnsley
S73 8QS

I understand that I will receive acknowledgement of my request within 5 days of receipt. My request will be completed within one calendar month in normal circumstances in accordance with the GDPR. However please note that The Trust will endeavour to complete your request as soon as is practical within this period

Office use only

Received by: Date:

Forwarded to: Date:

Date to be completed by:

Comments:

Appendix G - Confidentiality and Data Protection Agreement 1

Every Child Matters Academy Trust agrees to the service operating a confidential service on our premises. Discussions between individual pupils and staff of will remain confidential unless the young pupil of sufficient maturity* agrees to sharing, or there is an over-riding duty of care to the young person or someone else.

Pupils will be made aware of the confidential nature of this service by staff of at their interventions. Pupils will also be asked by staff of if, and what they may wish to share with the school, their parents or any third parties and their wishes will be respected.

Every Child Matters Academy Trust is registered with the Information Commissioners Office for Data Protection purposes. Every Child Matters Academy Trust takes the security of pupil data seriously and expects agency to implement appropriate security and other measures to safeguard pupils and their data in line with data protection legislation.

Confidentiality and data handling will form part of the review of this Service Level Agreement. Any concerns in this regard will be addressed by the personnel from each organisation.

Signed on behalf of Every Child Matters Academy Trust:

Name (please print):

Role:

Date:

Signed on behalf of

Name (please print):

Role:

Date:

Appendix H - Confidentiality and Data Protection Agreement 2

Every Child Matters Academy Trust agrees to the service operating a service on our premises. Every Child Matters Academy Trust recognises that offers a confidential service in normal circumstances. However the service, when delivered on our premises, will be done so in line with the school's policy on confidentiality. The school will normally share information about the pupil's progress with the parent. It is only in exceptional circumstances where a conflict of interest may exist will the school consider withholding information. The service when working with pupils on our premises will adhere to this 'open' policy.

Discussions between individual pupils and staff of may be shared with the school and parents unless it is agreed that an exception can be made in a particular circumstance involving a pupil of sufficient maturity.*

Pupils/parents will be made aware of the open nature of this service by staff of at their interventions.

Every Child Matters Academy Trust is registered with the information Commissioners Office for Data Protection purposes. Every Child Matters Academy Trust takes the security of pupil data seriously and expects agency to implement appropriate security and other measures to safeguard pupils and their data in line with data protection legislation.

Confidentiality and data handling will form part of the review of this Service Level Agreement. Any concerns in this regard will be addressed by the personnel from each organisation.

Signed on behalf of Every Child Matters Academy Trust:

Name (please print):

Role:

Date:

Signed on behalf of:

Name (please print):

Role:

Date:

Sufficient maturity*

The Information Commissioner would regard a young person age 12 to be of sufficient maturity to exercise their rights under the Data Protection Act. This includes the right to Consent or withhold consent to share. This is a general guide and it is recognised that some younger people may be sufficiently mature whereas some older people may not.

Appendix I - CCTV Signage Advice

All signs should be clearly visible and legible to members of the public. The size of signs will vary according to circumstances. For example:

- A sign on the entrance door to a building office may only need to be A4 size because it is at eye level of those entering the premises.
- Signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large (probably A3 size) as they are likely to be viewed from further away, e.g. by a driver sitting in a car.

The signs should contain the following information:

- Identity of the person or organisation responsible for the scheme.
- The purposes of the scheme.
- Details of whom to contact regarding the scheme.

Appendix J - CCTV Operational Checklists

Introduction

This checklist is designed to help operators of small CCTV systems comply with the legal requirements of the GDPR 2018 and it details the main issues that need to be addressed when operating a CCTV system. When used as part of a regular review process it should help to ensure that the CCTV system remains compliant with the requirements of the Act.

It is important that the Data Protection Act is complied with because failure to do so may result in action being taken under this Act. Failure to comply with Data Protection requirements will also affect the police's ability to use the CCTV images to investigate a crime and may hamper the prosecution of offenders.

If you use a CCTV system in connection with your school you should work through the checklist and address all the points listed. This will help to ensure that your CCTV system remains within the law and that images can be used by the police to investigate crime.

Small User Checklist

Operation of the CCTV System;

This CCTV equipment and the images recorded by it are **controlled by** who is responsible for how the system is used and for the notifying the Information Commissioner about the CCTV system and its purpose (this is a legal requirement of the GDPR 2018).

The above controller has considered the need for using a CCTV system and has decided it is required for the prevention and detection of crime, for protecting the safety of the school and for the general running of the school. It will not be used for any other purposes.



Description	Checked (Date)	By	Date of Next Review
The controller is aware that notification to the Information Commissioner is necessary and must be renewed annually			
Notification has been submitted to the Information Commissioner and the next renewal date recorded			
Cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are signs showing that a CCTV system is in operation visible to people visiting the premises and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system.			
The recorded images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained for 14 days to allow any incident to come to light (e.g. for a theft to be noticed).			
Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties.			
The operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment such as the date and time stamp are correctly set).			
Controller Knows how to respond to requests from individuals for access to images relating to that individual. See CCTV Code of Practice			

Appendix K - Photograph/Video/Artwork/Activities Consent and Release

Occasionally we may take photographs of children at our school. We use these images as part of our school displays and class projects and sometimes in other printed publications and social media. To comply with the Data Protection Act we need your permission before we can photograph or make any recordings of your child.

Please complete and sign the form below, and return to the school:

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear on the school's website

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear on school displays and class projects. Occasionally we may wish to publish a name with a photograph on a school display only - I consent/do not consent for my child's name to be used on a school display.

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear on the school's facebook page.

I consent/do not consent (delete as appropriate) for my child's photograph to appear in the media.

I consent/do not consent (delete as appropriate) for my child to have a school photograph taken. I understand this printed/digital photograph can be purchased by parents.

I consent/do not consent for my child to use the internet in line with school's acceptable usage policy (policy shown on school website)

I consent/do not consent for my child to view film and video clips rated PG

I consent/do not consent for my child to take part in food preparation/cooking/tasting

I consent/do not consent for my child to attend supervised walks in the local area

Name of child:

Name of parent/guardian:

Signature of parent/guardian

Date:

Please note you may alter this consent at any point by completing a new form. Please note there is no detriment to your child if consent is refused.

Appendix L - Parents who wish to use photography and/or video at a school event

Please note whereas this issue is not subject to the Data Protection Act schools need to have guidelines in place to cover such events. The following are guidelines which the schools might wish to adopt.

Generally photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves.

By following some simple guidelines we can proceed safely and with regard to the law. Remember that parents/carers and others, attend school events at the invitation of the Head teacher.

The Head teacher has the responsibility to decide if photography and videoing of school performances is permitted

The Head teacher has the responsibility to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.

Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photos and videos must not be sold and must not be put on the public facing social media networks.

Recording or/photographing other than for your own private use would require the consent of all the other parents whose children may be included in the images.

Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

Parents and carers must not photograph or video children changing for performances or events. If you are accompanied or represented by people that school staff do not recognise they may need to check who they are, if they are using a camera or video recorder.

Remember that for images taken on mobiles phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.

In exceptional circumstances e.g. child protection orders the parent and Head teacher may agree an alternative and practical approach to this policy for specific pupils.



Every Child Matters Academy Trust
Children at the heart

Appendix M - DATA COLLECTION FORM

Child's name		Date of Birth:	
Home address:			
		Post Code:	
Previous school / Nursery if applicable:			

Details of Parents/Guardians

Parent 1

Full name		Priority *:	
Home address:			
		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	
Email Address:		Parental responsibility? Yes / No	

Parent 2

Full name		Priority *:	
Home address:			
		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	
Email Address:		Parental responsibility? Yes / No	

*Note - the priority order someone should be contacted in the case of an emergency in school
(ie: 1st, 2nd, 3rd, 4th etc)

The school runs a text message service. The Priority #1 contact will receive relevant messages in the event of an emergency or school closure. Please tick the box to confirm you **wish to receive SMS** text messages. "

Emergency contact numbers alternative to parents/guardian

Emergency Contact 1 Relationship to child: _____

Full name		Priority *:	
Home address:			
		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	

Emergency Contact 2 Relationship to child: _____

Full name		Priority *:	
Home address:			



Every Child Matters Academy Trust
Children at the heart

Post Code:

Home telephone:

Mobile:

Day / Work Telephone:

Emergency Contact 3 Relationship to child: _____

Full name

Priority *:

Home address:

Post Code:

Home telephone:

Mobile:

Day / Work Telephone:

Do any of the following apply? Please attach a copy of legal document(s) if applicable

Adoption

☐

Court Order

☐

Residency Order

☐

Special Guardianship

☐

Any other Restrictions (please provide details)

☐

Details of any other Restrictions:

Medical Information

Doctors

Doctors address

Doctors phone No.

Medical conditions

My child has NO current medical needs

☐

My child has a medical condition, or is undergoing investigations (please complete a **Medical Information Collection Form** available in school office).

☐

Special Needs

Does your child have any special needs? Yes / No (please delete as appropriate)

Ethnicity

Country of birth: _____

Nationality _____

1st Language _____

Ethnicity

White British

White Irish

Other white
background

M – white &
black Caribbean



Every Child Matters Academy Trust
Children at the heart

M - White & Black African		M -White & Asian		M –any other		AAB -Pakistani	
AAB Bangladeshi		AAB - Indian		AAB - any other		BBB - Caribbean	
BBB - African		BBB – any other		Chinese		Arab	
Other ethnicity:		I do not want an ethnic background to be recorded					
M = Mixed AAB = Asian or Asian British BBB = Black or Black British							

Sibling information (if any)

Name	School
1.	
2.	
3.	

I/We consent to the school (through the head as the person responsible) obtaining, using, holding and disclosing “Personal data” including “sensitive personal data” (such as medical information), for the purposes of safeguarding and promoting the welfare of our child, and where necessary, for the legitimate interests of the School and ensuring that all relevant legal obligations of the school and ourselves are complied with. I/ We give my/our consent to such processing and disclosure provided that at all times any processing or disclosure of personal data or sensitive personal data is done lawfully and fairly in accordance with the Data Protection Act 1998.

Signature Date

Appendix N - Audit Outline

1. Aims of Data Protection Compliance Audits

1. Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
2. Quality Assurance, ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
3. Retention, appropriate weeding and deletion of information.
4. Documentation on authorised use of systems, e.g. codes of practice, guidelines, etc.
5. Compliance with individual's rights, such as subject access.
6. To assess the level of compliance with the organisation's own data protection system.
7. To identify potential gaps and weaknesses in the data protection system.
8. To provide information for data protection system review.

2. Audit Objectives

When carrying out a Data Protection Audit in any area of an organisation the Auditor has three clear objectives:

1. To verify that there is a formal (i.e. documented and up-to-date) data protection system in place in the area.
2. To verify that all the staff in the area involved in data protection:
 1. Are aware of the existence of the data protection system;
 2. Understand the data protection system;
 3. Use the data protection system.
3. To verify that the data protection system in the area actually works and is effective.

3. Areas to be examined include:

4. Use of appropriate forms when collecting data.
5. Storage of data in accordance with the security policy, e.g. locked cabinets, passwords, etc.
6. Data being removed in accordance with policy timescales.
7. Subject Access Request process in place.
8. CCTV compliance. Checklist completed and sent to the Data Protection
 - Officer at Head Office.
 - Staff training requirements assessed and highlighted.



Appendix O - Audit Return

School:

Date:

Description	Current Situation	Status	Action	Owner	Deadline
Staff/Pupil Records					
Student data is kept in accordance with the data retention policy					
Staff data is kept in accordance with the data retention policy					
Expired records are disposed of safely and securely by named individuals					
All forms used to collect data are identified					
All forms used to collect data include the standard ECM Data Protection disclaimer					
The pupil data collection sheet is sent out to parents annually at a set time to collect/refresh pupil data					
All electronic databases in use including the users who can access them are identified					
Access to all electronic databases is secured by individual username and password					
All paper record systems in use for staff or pupils are identified					
All paper systems are secured in accordance with policy guidelines					
Staff with access to staff records is documented					



controlled and regularly reviewed					
The accident book is used for pupils and records are kept for 40 years from the date the incident is logged					
All pupils whose parents have opted not to have their photograph used are clearly identified with the information easily accessible by staff					
All third party organisations offering a service on your premises including the data they collect are identified.					
All service level agreements with third party organisations are reviewed to consider data handling compliance.					
ALL CCTV Systems installed on your premises (if any) are documented.					
Appropriate CCTV signage is in place?					
The CCTV checklist is completed annually and returned to the data protection officer					
The school has a policy in place regarding the use of photography/video by family members at events. The method and frequency of communicating this to parents is documented and completed					
Contact details of parents are not distributed to other parents, for legitimate school activities, unless a signed parent Consent Form is received by the school					



A subject access request (SAR) file is in place to store requests					
THE SAR Process has been tested. Please complete Appendix D for a random pupil to test the process and outline any issues or concerns					
Staff Training					
Staff are made aware of ECM's Data Protection Policy and its implications for them in their work.					
Staff are made aware of ECM's acceptable use of ICT, mobile devices and networking sites policy and its implications for them in their work.					
Staff are made aware of that they must inform the school of any changes to their personal details e.g. change of address, contact numbers					
Have all staff had the minimum training session and been given the DO and Don't list? If not when is this planned?					

Status Key

Status	Description
	Policy Standard Not Met
	Policy standard partially met. Action plan in place to achieve full compliance
	Policy Standard achieved

Audit completed by (Print name):

Signed:

Position:

Date:

Appendix P - Data Retention Guide

1. Purpose of the Data Retention Guide

In the course of its activities every school creates and receives a large amount of information. Much of this information contains personal data which is in turn subject to the GDPR 2018 .

Personal data is any information relating to a living individual and would include information on pupils, members of staff and other employees. Data is very widely construed and can include internal files, letters, faxes, memoranda and notes, email, computer data and even voicemail, SMS and CCTV images created or received in the course of your operations.

This guide is intended to apply across the ECM group of schools to all data received and held whatever format that data is held in.

It is extremely important that data is held for the correct period of time so as to be available for the proper needs of the school. Indeed some classes of data are required by law or good business practice to be kept for a specified period of time and failure to do so may at best prejudice the position of ECM schools and at worst expose the group or its staff and employees to potential lawsuits and/or fines or even put them in contempt of court. However, keeping all data for an unlimited period of time will not only be impractical but will also expose ECM schools to risk under the DPA. This is because the retention of unnecessary data will create a compliance risk under the DPA as this requires that personal data is:

- Adequate relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary

The excessive storage of data is not only highly obstructive to the smooth operation of the school but will also create a risk of prejudicing some or all of the above data protection principles. The purpose of this guide is to provide guidelines for the retention, storage and disposal of the data held by the school.

2. Retention Periods

Except as otherwise indicated in accordance with paragraph 4 below data should be retained for the number of years indicated in the Retention Schedule below.

Each school will be responsible for the implementation of this guide. It is acknowledged that each school may currently have its own specific requirements and procedures for processing, storage and retention of data. These specific requirements and procedures should be reviewed against this guide to ensure that they are consistent with the procedures and time period specified in this guide. Any conflict or contradiction between a procedure which is specific to school and this guide should be discussed with the Data Protection Officer.

Where, in accordance with paragraph 4, it is necessary for a school to retain certain data for a period beyond the period indicated in the schedule, the school will maintain a flagging process to identify those records which must be retained beyond the specified period. The flagging process employed will be dictated by the records system in use. Unless a flag has been given in respect of specific data then data should be destroyed as soon as practicable after expiry of the specified retention period.

3. Disposal of Records

A document which is to be destroyed in accordance with this guide is likely still to be sensitive in the wrong hands, to deal with confidential or personal matters and/or have other security implications. The method by which these types of documents are disposed is of importance both because of the inherent risk such material falling into the wrong hands and because in accordance with Principle 7 of the DPA, ECM schools has a legal duty to ensure that it is disposed of securely. The method of disposal of data shall be consistent with the type of data being destroyed. Confidential data should be disposed of in a way that prevents the data from being accessible to others.

The main disposal methods and safeguards are as follows:

- Secure destruction and recycling by specialised firms. The security of the service provider's methods should be fully investigated and guarantees built into any contract where possible.
- Shredding. For highly sensitive documents some types of shredding may not be sufficient and the waste may itself need to be destroyed in order to ensure that it cannot be pieced back together (this would be far more difficult if a quality cross-cut shredder was used). If shredding is done centrally, consideration may need to be given to the security of documents awaiting destruction.
- Incineration. Consideration will need to be given to environmental and other safety implications.
- Overwriting electronic data, or otherwise making it unreadable. Care needs to be taken to ensure that sensitive data is completely erased. For example, deleting a file on a PC may only delete the file reference and not the underlying data. With the right tools and knowledge, it is possible to reconstruct the file. Great care should also be taken to ensure the secure disposal of physical IT equipment upon which the personal data may have been held or processed.

4. Archiving data

In general once data or documents are no longer "live" they should be moved to archiving as soon as is reasonably possible. Archiving should not be confused with destruction. You need to keep in mind that archived data and documents carry with them on-going obligations and are subject to the requirements of the DPA, for instance, archived data and documents will need to be considered in the event of any subject access request and the archiving system must be kept properly secure.

Data and documents which have been archived should be reviewed against the criteria set out in this guide with a view to destruction after the relevant time period. Ultimately the archival period for data and documents is a matter of balancing costs of holding the data or documentation in archive which is highly unlikely ever to be needed against the general principle that everything else being equal, and it is better to be safe than sorry.

5. Retention of Data beyond the Retention Period

Where data should be retained indefinitely:-

(1) If you receive notice of any lawsuit, government or regulatory investigation (for instance, health & safety investigations), other legal action, complaint or claim against or involving ECM Schools, the School or any member of staff, or employee, or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation complaint or claim, then you should flag all data which may be relevant for preservation in respect of the same. Any data so flagged shall be preserved and shall not be destroyed

(2) If any member of staff or employee becomes aware that any notice has been received by the school of any lawsuit, government or regulatory investigation, other legal action, complaint or claim against or involving ECM, the school or any member of staff, employee or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation, complaint or claim, that member of staff or employee should immediately notify the school's Data Protection Officer in order that the Officer can review which data should be [flagged] for extended retention in accordance with this guide. The member of staff or employee must not destroy any data relevant to such action, proceeding, investigation, complaint or claim whether it not it would otherwise fall to be destroyed in accordance with this guide.

(3) If any member of staff or employee is unsure whether any unflagged data is relevant to an action, proceeding, investigation complaint or claim the member of staff or employee should not delete that data and should liaise with Data Protection Officer.

Once data has been flagged all members of staff and employees must preserve and prevent the destruction of any such data (including e-mails and other computer records).

Destruction of such data, even if inadvertent, could seriously prejudice the member of staff or employee, the school and ECM and could subject the individual, the school and ECM substantial criminal and civil liability including fines and other penalties.

Whenever data is flagged the data shall be preserved until the flag is removed. The communication imposing the [flag] shall be stored with the preserved data until that flag is removed, following which the data shall be destroyed as soon as reasonably possible.

6. Violations

Due to the potentially serious consequences of a violation of the procedures set out in this guide any violation may be subject to disciplinary action.

All members of staff or employees should report any suspected violations of this guide to the Data Protection Officer.

7. Questions

Anyone with questions about this guide should contact their *Data Protection Officer*.

Remember:

Data we record about individuals (staff, pupils, parents etc.) is covered by the Data Protection Act and belongs to that individual. As such, notes we make on SIMS, PORTAL, in emails and paper records may be seen by the person concerned.

We have access to data as part of our role within the school. This data should not be disclosed or used for any purpose that is not official business of the school.

The school has a data protection officer who can provide advice in case of uncertainty.

Here is a list of 'top tips' when handling school data.....

DO ✓

- Record facts and professional opinions only, on school records, emails and other similar documents
- Use a strong password on I.T. Systems at work, e.g. a combination of 8 or more alphanumeric characters and symbols.
- Change passwords on a regular basis.
- Password protect email attachments containing personal or commercially sensitive data.

- Encrypt any removable data devices including USB sticks laptops and similar.
- Remember the school may incur substantial fines for loss or misuse of data.
- Read and familiarise yourself with the Acceptable Use Policy (I.T.).
- Keep data secure when using it off site.
- Think security when posting sensitive documents.

DON'T x

- Use personal social media with pupils.
- Contact pupils or store pupil/parent contact data on personal devices, e.g. numbers on your mobile.
- Use your mobile phone outside designated areas in school.
- Don't share passwords.
- Don't leave personal data unattended when off site.
- Don't create databases of Personal Data in addition to the official sources e.g. SIMS and PORTAL.

Taking data off site.

- only take offsite, information you are authorised to and only when it is necessary.
- ensure that it is protected offsite by not leaving it unattended,
- locking it away when not in use,
- not discussing or sharing it with non-school staff.
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any online services you have used e.g. email
- try to avoid other people seeing the information you are working with
- treat records as if they were your bank details and PIN



Appendix Q – Data Sharing Approval & Assurance Record

1. Arrangement / request	
Organisation(s) receiving data	
Purpose of sharing	
Pupil cohort / individuals covered	
Data fields to be shared	
Method / system used for sharing	
Who can access the information	
Wider pupil data accessible?	☐ No ☐ Yes – details: _____
DPIA / EIA	☐ Obtained ☐ Reviewed ☐ Action required
Data / Information Sharing Agreement	☐ Obtained ☐ Reviewed ☐ Action required
Lawful basis – Article 6	
Statutory power / duty / gateway	
Article 9 / DPA 2018 condition (if applicable)	
Privacy notice	☐ Checked ☐ Update required
ROPA / data map	☐ Updated / cross-referenced ☐ Action required

ECM APPROVAL CONDITION

Approval is limited to the purpose, pupil cohort, data fields, recipients and system permissions recorded above. Any material change must be referred to ECM centrally before approval.

1. Data minimisation / proportionality	☐ Satisfied ☐ Action required
Security / access controls	☐ Satisfied ☐ Action required
Supporting documentation retained	☐ Satisfied ☐ Action required
Overall decision	☐ APPROVED ☐ APPROVED WITH ACTIONS ☐ NOT APPROVED

SIGN-OFF & REVIEW

DPO / Data Protection Lead		Date	
Senior Trust approval		Date	
Next review date		Review trigger	Material change / incident / annual review

Supporting evidence retained / location:



Appendix R - Disposal Log

Date	Description	Records Included	Exception
	<i>Example: Annual audit of records in line with retention timescale or request from subject to change or delete record</i>	<i>Records reaching D.O.B + 25 year rule</i>	<i>Individual Pupils Record as per retention log e.g. for legal proceedings ongoing etc.</i>