The Circle Trust Document: Data Protection Policy including Freedom of Information

Author:	Executive Headteacher
Approver:	Trustees
Owner:	School Improvement Committee
Date:	14 December 2020
Next review:	January 2023

Changes History:

Version	Date	Amended by:	Substantive changes:	Purpose
1.0	20.9.17	Exec Head	New Document	First release
1.1	03.05.18	AH	Amended in light of the new GDPR regulations	To meet new regulations
1.2	4.10.18	AH	Policy refreshed in light of first year of operation and re-adding FOI section including Data Publication Scheme	Compliance
1.3	28.1.20	AH	IRMS guidance updated and attached. Email guidance clarified	Compliance
1.4	29.10.20	AH	Appeals for SARs within the Trust Email retention amended Photo retention introduced Addition of Biometric section New Appendix for special categories of data	Compliance and improvement to current practice

Purpose of the Policy

1.1 The Circle Trust recognises and accepts its responsibilities to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and the General Data Protection Regulation (GDPR) in the Data Protection Act 2018 and other related legislation. This applies to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All employees involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines

1.2 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.3 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.4 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.5 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 **Introduction**

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

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

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

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

3 **The Aims and Objectives of Data Protection**

3.1 The Trust's overall data handling and protection approach is to:

3.1.1 Protect children and young people, staff, assets and reputation from harm

3.1.2 Have all data handling and protection responsibilities clearly defined, assigned and communicated

3.1.3 Ensure that all employees are aware that they have a duty to protect data

3.1.4 Ensure compliance with the statutory requirements

3.1.5 Anticipate and respond to changing legislative requirements and adopting legal compliance as a minimum standard

3.2 These aims and objectives will be achieved by:

3.2.1 Maintaining accurate, compliant documented procedures for data protection control

3.2.2 Providing suitable information, training and supervision

3.2.3 Maintaining effective communication and the active involvement of all staff

3.2.4 Maintaining an appropriate incident reporting and recording system, with investigation procedures to establish cause and prevent recurrence

3.2.5 Monitoring arrangements

4 Definition of data protection terms

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

5 The management of Data Protection

5.1 The Trustees have a fundamental role to:

5.1.1 Ensure this policy is compliant to Data Protection legislation.

5.1.2 Regularly review this policy to approve changes or improvements to key elements of its processes and procedures

5.1.3 Be satisfied that Data Protection arrangements are actively managed, with the appropriate controls in place and working effectively

5.1.4 Review breaches in Data Protection.

5.1.5 Appoint a Trustee with responsibility for Data Protection

5.2 The Executive Headteacher will:

5.2.1 Implement this policy

5.2.2 Operationally lead, monitor and review all matters relating to Data Protection.

5.2.3 Provide Headteachers with guidance, interpretation and understanding of the risk in relation to Data Protection including responsibilities to display privacy notices and publication schemes.

5.2.4 Provide a mechanism for data handling and data protection management issues to be discussed and disseminated to all areas of the Trust

5.2.5 Audit and review local school arrangements in relation to Data Protection to ensure compliance

5.2.6 Appoint a Data Protection Officer

5.2.7 Ensure that each school within the Trust has appointed a Data Lead

5.2.8 Ensure that there is a recovery strategy for data loss

5.2.9 Report Data Protection incidents or infringement to Trustees particularly with regard to the nature, extend and affect of any loss of data.

5.3 The Local Advisors have a fundamental role to:

5.3.1 Be satisfied that Data handling and protection is actively managed, with the appropriate controls in place and working effectively in their school

5.3.2 Receive a termly Data Protection update

5.3.3 Review breaches in Data Protection affecting their school

5.4 A Headteacher with the oversight of Local Advisors will:

5.4.1 Have primary responsibility for managing Data Protection in their school on a day-to-day basis

5.4.2 Create, regularly review and publish their school's Data Publication Scheme

5.4.3 Ensure privacy notices for parents/carers/child and young people and employees and publication schemes are displayed on the school website

5.4.4 Follow the procedures laid out in this policy in respect to Subject Access Request ensuring where possible a full response within one month under GDPR to requests for information and data.

5.4.5 Be responsible for school Data Protection breaches, issues or concerns and to response and co-operate with the Information Commissioners Office.

5.4.6 Have responsibility for promoting good data handling practice, 'privacy by design' and data protection procedures within day to day operations including regular training for staff

5.4.7 Ensure that Data Protection management becomes a regular Local Advisor meeting item

5.4.8 Ensure that Data Protection management is incorporated at the conceptual stage of any project as well as throughout a project

5.4.9 Report concerns or early warning indicators and/or any Data Protection breaches to their Local Advisors, the Executive Headteacher and Chief Finance Officer

5.4.10 Will appoint a Data Protection Lead for their school, to lead on all matters for data protection in that school.

5.4.11 Data will only be retained in school for as long as is necessary. As there are no current guidelines from the DfE for retention of data, the Trust will follow the recommendation set out by the Information and Records Management Society (IRMS) toolkit. See Appendix 1.

5.4.12 Ensure that all data when destroyed is deleted securely. Personal data on paper must be shredded and electronic data shredded with appropriate software.

6 Data Protection Officer

6.1 As a Trust, we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Andy Hinchliff, and he can be contacted at andy@thecircletrust.co.uk

6.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

6.3 The Data Lead in each school is the central point of contact for all **data subjects** in that school and others in relation to matters of data protection.

6.4 The DPO is the point of contact for all Data Leads and for the Information Commissioners office (ICO).

7 Data protection principles

7.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

7.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

7.1.2 **Processed** for specified, lawful purposes and in a way which is compatible with those purposes;

7.1.3 Adequate, relevant and not excessive for the purpose;

7.1.4 Accurate and up to date;

7.1.5 Not kept for any longer than is necessary for the purpose; and

7.1.6 **Processed** securely using appropriate technical and organisational measures.

7.2 **Personal Data** must also:

7.2.1 Be **processed** in line with **data subjects'** rights;

7.2.2 Not be transferred to people or organisations situated in other countries without adequate protection.

7.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust

8 Fair and lawful processing

8.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

8.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

8.2.1 That the **personal data** is being **processed**;

8.2.2 Why the **personal data** is being **processed**;

8.2.3 What the lawful basis is for that **processing** (see below);

8.2.4 Whether the **personal data** will be shared, and if so with whom;

8.2.5 The period for which the **personal data** will be held;

8.2.6 The existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

8.2.7 The right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

8.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

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

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

8.4.2 Where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);

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

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

8.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. See Appendix 4. We will normally only **process special category personal data** under following legal grounds:

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

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

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

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

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

8.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

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

Consent

8.9 Where none of the other bases for **processing** set out above applies then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

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

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

8.12 In relation to all pupils under the age of 13 years old, we will seek consent from an individual with parental responsibility for that pupil.

8.13 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

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

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

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

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

8.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

8.16 The DPO or Data Lead must always be consulted in relation to any consent form before consent is obtained.

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

9 Processing for limited purposes

9.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

9.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

10 Notifying data subjects

10.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

10.1.1 Our identity and contact details as **Data Controller** and those of the DPO;

10.1.2 The purpose or purposes and legal basis for which we intend to **process** that **personal data**;

10.1.3 The types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

10.1.4 Whether the **personal data** will be transferred outside the European Economic Area (‘**EEA**’) and if so the safeguards in place;

10.1.5 The period for which their **personal data** will be stored, by reference to our Retention Guidelines as set out in the IRMS 2019 Toolkit in Appendix 1;

10.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

10.1.7 The rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

10.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

10.3 The Trust will be provided with information relating to third parties in the form of emergency contact details. These individuals must be provided with the information above. Practically we suggest that parents are required to obtain the consent of any third party whose details they provide to the Trust for these purposes.

11 Adequate, relevant and non-excessive processing

11.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

12 Accurate data

12.1 We will ensure that **personal data** we hold is accurate and kept up to date.

12.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

12.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

13 Timely processing

13.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** that is no longer required.

13.2 We shall seek to comply with the rights exercised by data subjects as set out in section 14 below as soon as possible and within legal time limits. However, there may be instances where due to circumstances outside of the Trust's control this may not be possible e.g. where the School or Trust has been closed or is only partially operable. In such circumstances data subjects will be notified and provided details about the reason for the delay and when a response can reasonably be expected.

14 Processing in line with data subjects' rights

14.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

14.1.1 Request access to any **personal data** we hold about them;

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

14.1.3 Have inaccurate or incomplete **personal data** about them rectified;

14.1.4 Restrict **processing** of their **personal data**;

14.1.5 Have **personal data** we hold about them erased

14.1.6 Have their **personal data** transferred; and

14.1.7 Object to the making of decisions about them by automated means.

14.2 The Trust should carefully consider whether it takes any decisions about any individuals by automated means. This includes any decisions made solely by automated means, and which has a legal effect in relation to the individual. This might include, for example, a decision as to whether to employ an individual. It is unlikely that this would apply to a school as there is always likely to be an element of human intervention in any decision making. However careful consideration should be given to this issue, called Profiling.

The Right of Access to Personal Data

14.3 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the Trusts Subject Access Request Procedure.

14.4 As part of the Subject Access Request procedures, a data subject if unhappy with any element of the Trust's response to their request, can appeal to the Trust's DPO.

The Right to Object

14.5 In certain circumstances, **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking based on a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

14.6 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds, which override the rights of the **data subject**.

14.7 Such considerations are complex and must always be referred to the DPO or Data Lead upon receipt of the request to exercise this right.

14.8 In respect of direct marketing, any objection to **processing** must be complied with.

14.9 The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

14.10 If a **data subject** informs a school that **personal data** held about them by the school is inaccurate or incomplete then we will consider that request and provide a response within one month.

14.11 If we consider the issue too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

14.12 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances, we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

14.13 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

14.14 The Trust must restrict the **processing** of **personal data**:

14.14.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

14.14.2 Where the Trust is in the process of considering an objection to processing by a **data subject**;

14.14.3 Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and

14.14.4 Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

14.15 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

14.16 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

14.17 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

14.17.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

14.17.2 When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;

14.17.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;

14.17.4 Where the **processing** of the **personal data** is otherwise unlawful;

14.17.5 When it is necessary to erase the **personal data** to comply with a legal obligation; and

14.18 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

14.18.1 To exercise the right of freedom of expression or information;

14.18.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

14.18.3 For public health purposes in the public interest;

14.18.4 For archiving purposes in the public interest, research or statistical purposes; or

14.18.5 In relation to a legal claim.

14.19 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

14.20 The DPO must be consulted in relation to requests under this right, who will also ensure the requests are complied with, within the timeframe above.

Right to Data Portability

14.21 In limited circumstances, a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to other organisation.

14.22 If such a request is made then the DPO must be consulted.

15 Data security

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

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

15.3 Security procedures include:

15.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the Data Lead of the school, who will in turn report to the DPO.

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

15.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be completely cleaned of data when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

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

15.3.5 **Working away from the school premises – paper documents.** Data users must ensure that any confidential information taken off site must be secured and not made available to anyone not employed by the Trust.

15.3.6 **Working away from the school premises – electronic working.** Data users must ensure that any confidential information accessed off site must be secured by password such as from a secure network or security pass on a laptop. No data should be downloaded or stored on another device such as a home computer that may be accessed by other people not employed by

the Trust. For remote learning including live lessons, please refer to the schools procedures for safeguarding and data protection.

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

15.3.8 **Emails.** All emails should be securely and permanently deleted centrally by an IT manager after 3 years. However some emails may be stored securely for longer to meet other legal requirements.

15.3.9 **Photographs.** All photographs should be kept the period of time the student is at school and then for a reasonable time after they have left school.

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

16 Data Protection Impact Assessments

16.1 The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

16.2 In certain circumstances, the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies, which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

16.3 Each School will complete an assessment of any such proposed **processing** and has a template document, which ensures that all relevant matters are considered.

16.4 The Data Lead should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

17 Disclosure and sharing of personal information

17.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency "ESFA"], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

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

17.3 In some circumstances, we will not share safeguarding information. Please refer to our Safeguarding Policy.

17.4 Further detail is provided in our Schedule of Processing Activities.

18 **Disclosure of school or Trust information under Freedom of Information Act 2000**

18.1 The Freedom of Information Act 2000 (FOIA) requires all public authorities (including schools) to adopt and maintain a publication scheme.

18.2 Handling Freedom of Information Requests - The FOI Act permits access to all types of information, for example organisational charts, policies, procedures and all documents specified in the publication scheme. Any requests for information under the FOI Act received by a member of staff via email or as a paper copy must firstly be forwarded to the Business Manager who will liaise with colleagues to provide the information.

18.3 Under the Freedom of Information Act, any individual is able to make a request to the Trust or a school for information. They do not have to indicate why they want the information. An applicant is entitled to be informed in writing as to whether the information is held and to have the information communicated to them, or provided with an explanation why this cannot be done.

18.4 Any request made to the Trust or a school stating the name of the applicant, including an address for correspondence and describing the information required qualifies as a request for information.

18.5 Timescale for Compliance - On receipt of a request the Trust or a school is obliged to inform the applicant in writing whether the information requested is held and if so, communicate that information to the applicant promptly, but not later than 20 working days after receipt of the request.

18.6 A request is received when it is delivered to the Trust or a school, or when it is delivered to the email inbox of a member of staff. The date of receipt is not the date the request is passed to the appropriate person for processing.

18.7 In respect of emails, however, where an automated 'out of office' message provides instructions on how to re-direct a message, the request would not be 'received' until it was resent to the alternative contact.

18.8 The correspondence to the applicant must state:

18.8.1 Whether the school holds the information of the type requested;

18.8.2 Whether it cannot be supplied due to the constraints of the Data Protection Act which takes precedence over any FOI rights;

18.9 If the information is held and can be provided it must be given to the individual in so far as possible in the format requested i.e. hard copy or electronic.

18.10 The Data and Admissions Manager (for the Trust) or the Business Manager (for a school) in conjunction with other appropriate school staff will collate information. Records of FOI requests and how they have been dealt with should be maintained by the school.

18.11 Exemptions and Exceptions - In certain circumstances the school may refuse a FOI request:

18.11.1 When the request is vexatious or repeated;

18.11.2 When the cost of compliance exceeds the appropriate limit (currently £450);

18.11.3 When the information falls under one of the exemptions.

18.12 Some information is exempt from disclosure and so does not have to be provided. There are two broad categories of exemptions:

18.12.1 Absolute exemptions. These are cases where the right to know is wholly disapplied. In some cases, there is no legal right of access at all, for instance information supplied by or relating to bodies dealing with security matters or information covered by parliamentary privilege. In other cases, for instance information available to the applicant by other means or personal information relating to the applicant, it may be possible to obtain the information by alternative means and not under the FOI Act.

18.12.2 Qualified exemptions. These are cases where the school, having identified a possible exemption, must consider whether the public interest in maintaining the exemption is greater than that in confirming or denying the existence of the information requested and providing the information to the applicant. The School Improvement Committee will consider all cases of possible qualified exemptions.

18.13 Exemptions are subject to the public interest test unless FOI states that they are absolute exemptions.

18.14 When applying the test the school is simply deciding whether in any particular case it serves the interests of the public better to withhold or to disclose information.

18.15 Should the Trust or a school receive a request for information, which is covered by an exemption, the applicant will be informed wherever possible within 20 working days of receipt of the request that the information cannot be provided together with an explanation. Where the school does not hold the requested information then again this must be communicated within 20 working days giving a brief explanation of why this is not held if appropriate and similarly where the applicant may find the information.

18.16 Vexatious and Repeat Requests - A request can be treated as vexatious where it would impose a significant burden on the school in terms of expense or distraction and meets at least one of the following criteria:

18.16.1 It clearly does not have any serious purpose or value;

18.16.2 It is designed to cause disruption or annoyance;

18.16.3 It has the effect of harassing the school;

18.16.4 It can otherwise fairly be characterised as obsessive or manifestly unreasonable.

18.17 Each specific request should be looked at and assessed individually.

18.18 The school will not normally refuse a request for information which should be available through the publication scheme on the grounds that it is vexatious. Issues of vexatious may arise where the school receives requests from individuals who have previously registered a grievance, pursued a complaint or otherwise been involved in a dispute. It is not unusual for those who believe they have been unfairly treated by the school to pursue or attempt to reopen their grievance by using the FOI.

18.19 Any request considered to be vexatious will be passed to the Data and Admissions Manager. Should this be linked to a complaint/dispute this will then be referred to the Headteacher.

18.20 All refusals for information will be communicated to the applicant in accordance with the paragraph above on exemption

18.21 Fees - The school will not levy a fee for FOI requests that are relatively straightforward and where the information held is readily available. Requests for information may be chargeable if significant staff time or resources will be required to meet the request. If a fee is chargeable then this will be agreed with the applicant before the request is processed.

18.22 The Government has published the FOI fees regulations. In accordance with this legislation fees are capped at £450. As a result, the Trust or a school may refuse to accede to a request for information if the cost of doing so is likely to exceed this amount.

18.23 The Circle Trust follows the template produced by the Information Commissioners Office and can be found at https://ico.org.uk/for-organisations/education/

18.24 Each school should publish the Circle Trust Data Publication Scheme on their website. See Appendix 2.

19 Data Processors

19.1 We contract with various organisations who provide services to the Trust, such as payroll providers, school meal providers and management information systems.

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

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

19.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

20 Images and Videos

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

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

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

20.4 As a Trust (and each school), we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

20.5 Whenever a pupil begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

20.6 In the event of teachers in the Trust using live streaming, each member of staff will follow the procedures laid down by each school. The Trust does not give permission for any third party recording lessons.

21 CCTV

21.1 Each school operates a CCTV system. Please refer to The Circle Trust CCTV Policy.

22 Biometric Data

22.1 The Trust operates a biometric recognition system for the purposes of:

22.1.1 payment of dinner monies

22.2 Before we are able to obtain the Biometric Data of pupils or the Workforce we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

22.3 For the Workforce, written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of your Biometric Data is received from the individual.

22.4 For pupils under the age of 18 years, the school will notify each parent of that pupil (that the School has the contact details for and is able to contact) prior to them commencing their education at the school of the use of our Biometric Recognition System. The School will then obtain the written consent of one of the pupil's parent before obtaining any Biometric Data.

22.5 In the event that written consent cannot be obtained from a parent, or any parent objects in writing or the pupil objects or refuses to participate in the processing of their Biometric Data, the Trust will not process the pupil's Biometric Data and will provide the following alternative means of accessing the above services:

22.5.1 providing a pin number

22.6 Further information about this can be found in our Notification of Intention to Process Pupil's Biometric Information (see appendix 3 below) and our Privacy Notices.

23 Changes to this policy

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

Appendix 1 – IRMS Toolkit Data Retention Guidelines

Appendix 2 – Data Publication Scheme

Appendix 3 - Notification of Intention to Process Pupil's Biometric Information

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

Please complete this form if you consent to the school taking [and using information from your child's [insert biometric – e.g. fingerprint] by [name of school] as part of an automated biometric recognition system. This biometric information will be used by [name of school] for the purpose of [describe purpose(s) for which this data will be used, e.g. administration of school/college library/canteen].

In signing this form, you are authorising the school to use your child's biometric information for this purpose until he/she either leaves the school or ceases to use the system. If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school at the following address:

[insert address]

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school.

Having read guidance provided to me by [name of school], I give consent to information from the [insert biometric – e.g. fingerprint] of my child:

[insert name of child] being taken and used by [name of school] for use as part of an automated

biometric recognition system for [describe purpose(s) for which this data will be used, e.g.

administration of school/college library/canteen].

I understand that I can withdraw this consent at any time in writing.

Name of Parent/Carer: ……..

Signature: ……

Date: ……

Please return this form to: [insert suitable delivery point and name of school].

Appendix 4 - Processing of special categories of personal data and criminal offence data

1. About this appendix

1.1. This appendix sets out how we will protect Special Categories of Personal Data and Criminal Convictions Data.

1.2. Where we process other Special Categories of Personal Data and Criminal Convictions Data in instances where there is no requirement to keep an appropriate policy document, we will process it on a basis that respects the rights and interests of Data Subjects. Further information in respect of this processing can be found within the Trusts privacy notices.

1.3. This appendix supports the Trust's Data Protection Policy and adopts its definitions and should be read in conjunction with that policy.

2. Why we process Special Categories of Personal Data and Criminal Convictions Data

2.1. We process Special Categories of Personal Data and Criminal Convictions Data for the following purposes where this is in accordance with our Data Protection Policy:

2.1.1. to carry out our legal obligations in relation to employment law;

2.1.2. for the purposes of preventative or occupational medicine in order to assess an employee's working capacity and/or the need for reasonable adjustments;

2.1.3. complying with health and safety obligations;

2.1.4. complying with the Equality Act 2010 and in the interests of ensuring equal opportunities and treatment;

2.1.5. checking applicants' and employees' right to work in the UK;

2.1.6. verifying that candidates are suitable for employment or continued employment;

2.1.7. to safeguard our pupils and other individuals;

2.1.8. to support individuals with a particular disability or medical condition;

2.1.9. to protect the data subject's vital interests where they are not able to provide their consent;

2.1.10. to prevent or detect crime without the consent of the data subject so as not to prejudice those purposes where it is necessary for reasons of substantial public interest; and

3. Personal data protection principles

3.1. The GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

3.2. We comply with the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

3.2.1. processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

3.2.2. collected only for specified, explicit and legitimate purposes (Purpose Limitation);

3.2.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

3.2.4. accurate and where necessary kept up to date (Accuracy);

3.2.5. not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and

3.2.6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

3.3. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4. Compliance with data protection principles

4.1. Lawfulness, fairness and transparency

4.2. Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.3. We will only Process Personal Data fairly and lawfully and for specified purposes. We will only Process Special Categories of Personal Data and Criminal Convictions Data where we have a lawful basis for Processing and one of the specific conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal basis and specific Processing condition relied on for each Processing activity below.

4.4. When collecting Special Categories of Personal Data and Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice setting out all the information required by the GDPR in a concise, transparent, intelligible, easily accessible manner and in clear plain language which can be easily understood.

Type of Special Categories of Personal Data/Criminal Convictions Data Processed	Lawful basis for Processing	Condition for processing Special Categories of Personal Data/Criminal Convictions Data
Data concerning health	Compliance with a legal obligation (*Article 6 (1)(c)*) or necessary for the performance of a contract with the Data Subject (*Article 6(1)(b)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.) Necessary for health and social care purposes. (*Paragraph 2(1), Schedule 1, DPA 2018*.) To provide support for individuals with a particular disability or medical condition. (*Paragraph 16(1), Schedule 1, DPA 2018*.) Necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially. (*Paragraph 17(1), Schedule 1, DPA 2018*.)
Racial or ethnic origin data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)
Criminal Convictions Data	Compliance with a legal obligation (*Article 6(1)(c)*). **OR** In the organisation's legitimate interests (*Article 6(1)(f)*) which are not outweighed by the fundamental rights and freedoms of the Data Subject.	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Controller or the Data Subject in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.) Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as:

		• preventing or detecting unlawful acts (*Paragraph 10(1), Schedule 1, DPA 2018*.) • protecting the public against dishonesty etc. (*Paragraph 11(1), Schedule 1, DPA 2018*.) • complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another persona has committed an unlawful act; or been involved in dishonesty, malpractice or other seriously improper conduct (*Paragraph 12(1), Schedule 1, DPA 2018*.) • preventing fraud or a particular kind of fraud (*Paragraph 14(1), Schedule 1, DPA 2018*.) Necessary for the purposes of: • protecting an individual from neglect or physical, mental or emotional harm, or • protecting the physical, mental or emotional well-being of an individual where the individual is under the age of 18, or is 18 or over and at risk. .(*Paragraph 18(1), Schedule 1, DPA 2018*.)
Equal opportunity data	In the organisation's legitimate interests (*Article 6(1)(f)*) which are not outweighed by the fundamental rights and freedoms of the Data Subject.	Necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained. (*Paragraph 8(1)(b), Schedule 1, DPA 2018*.)

4.5. Purpose limitation

4.5.1. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

4.5.2. We will only collect Personal Data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Notice. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law) we will check that this is compatible with our original purpose. [We will not use Personal Data for new, different or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

4.6. Data minimisation

4.6.1. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4.6.2. We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes. We will periodically review the Personal Data and delete anything we don't need.

4.7. Accuracy

4.7.1. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

4.7.2. We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

4.7.3. To check the accuracy of Special Categories of Personal Data/Criminal Convictions Data, each school will request parents/carers, students and staff to check their data such as medical data on an annual basis. This can be done via online portals or data collection sheets.

4.7.4. As set out in our Data Protection Policy, Data Subjects have the right to rectification. Our Data Protection Policy confirms how the Trust considers and complies with any request to the right to rectification.

4.8. Storage limitation

4.8.1. We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once

we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

4.8.2. We maintain a Data Retention Policy and related procedures to ensure Personal Data is deleted after it is no longer needed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

4.8.3. We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice and our Data Retention Policy.

4.9. Security, integrity, confidentiality

4.9.1. Personal Data shall be Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. We will analyse any risks presented by our Processing to assess the level of security required.

4.9.2. Each school will ensure that particular types of Special Categories of Personal Data/Criminal Convictions Data you are processing, only by staff who need to use the information and is securely stored.

4.10. Accountability principle

4.10.1. We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO. We also have appropriate data protection policies in place, such as privacy notices and retention policies.

4.10.2. We will:

4.10.2.1. Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.

4.10.2.2. Carry out a DPIA for any Personal Data Processing that is likely to result in a high risk to Data Subjects' interests to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.

4.10.2.3. Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.

4.10.2.4. Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with these principles.

4.11. Controller's policies on retention and erasure of personal data

4.11.1. We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed so that:

4.11.1.1. Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

4.11.1.2. Where records are destroyed we will ensure that they are safely and permanently disposed of.

4.11.2. Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period. The Privacy Notice [alongside our Data Retention policy] is also available on our website.

ANNEX

DEFINITIONS

Term	Definition
Criminal Convictions Data	personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Data Privacy Impact Assessment (DPIA)	tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.
Data Protection Officer (DPO)	as set out in our Data Protection Policy, as a Trust the person we have appointed to be responsible for ensuring compliance with the DPA 2018 and GDPR, as our DPO is Andy Hinchliff, and they can be contacted at andy@thecircletrust.co.uk .
Data Retention Policy	explains how the organisation classifies and manages the retention and disposal of its information. Time periods for retention are set out in the retention schedule.
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Data Users	are those of our workforce (including Trustees/Advisors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures

	at all times
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Privacy Notice	a separate notice required to be provided to Data Subjects which is usually given at the point the organisation collects information about them.
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Profiling	any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by the Trust such as staff and those who volunteer in any capacity including Trustees, Advisors, members or parent helpers.