Prinicpal
Anna Mansaray

Parkwood Hall
Co-operative Academy
Beechenlea Lane
Swanley
Kent
BR8 8DR

Telephone : 01322 664441
Fax: 01322 613163

PARKWOOD HALL
CO-OPERATIVE ACADEMY

Parkwood Hall
Co-operative Academy

"Growth through Personal and Social Learning "

Statutory Policy File

DATA PROTECTION

Index No: 28 (v2.0)

Parkwood Hall Co-operative Academy is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment'

Our Core Values

CONTENTS

1 STATEMENT OF INTENT 2
2 LEGAL FRAMEWORK 2
3 APPLICABLE DATA 3
4 PRINCIPLES 3
5 ACCOUNTABILITY 4
6 DATA PROTECTION OFFICER (DPO) 5
7 LAWFUL PROCESSING 5
8 CONSENT 6
9 THE RIGHT TO BE INFORMED 7
10 THE RIGHT OF ACCESS 8
11 THE RIGHT TO RECTIFICATION 9
12 THE RIGHT TO ERASURE 9
13 THE RIGHT TO RESTRICT PROCESSING 10
14 THE RIGHT TO DATA PORTABILITY 10
15 THE RIGHT TO OBJECT 11
16 PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS 12
17 DATA BREACHES 13
18 DATA SECURITY 13
19 PUBLICATION OF INFORMATION 15
20 CCTV AND PHOTOGRAPHY 15
21 DATA RETENTION AND DISPOSAL 16
22 DISCLOSURE AND BARRING SERVICE (DBS) DATA 16
23 RESPONSIBILITIES 17

DATA PROTECTION

Parkwood Hall is a Co-operative Academy and we have adopted the values of the co-operative movement to assist us as we govern the school. We have also developed values for learning and teaching that inspire our students and staff alike.

Our co-operative values are self help, self responsibility, democracy, equality, equity, solidarity, honesty, openness, social responsibility and caring for others. These are the ways in which we do things at our school and they sit at the heart of all our policy development.

In this policy the following values are particularly relevant:

- Honesty and openness – it is our duty to be open and transparent in our dealings with the public; including parents, families, suppliers and contractors. We aim to operate to the highest levels of probity and freedom from accusations of corrupt or underhand practice.
- Self-responsibility – each employee and trustee must monitor their own behaviour and that of their colleagues, to ensure that the highest standards of best practice are upheld, and to raise concerns (see the Whistleblowing Policy) without fear or favour.

1 STATEMENT OF INTENT

Parkwood Hall Co-operative Academy is required to keep and process certain information about its staff and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The School may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools, educational bodies, social services and possibly the police/solicitors.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the School complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Parkwood Hall believes that it is good practice to keep clear practical policies, supported by written procedures.

To ensure the full compliance with GDPR, all Staff receive data protection training and/or data protection information.

2 LEGAL FRAMEWORK

This policy has due regard to legislation, including, but not limited to the following:

- Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000

- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- DfE Data protection: a toolkit for schools (April 2018)

This policy will be implemented in conjunction with the following other School policies:

- E-safety Policy
- Teaching and Learning Policy
- Freedom of Information Policy

The Academy Business Manager is categorised as a Data Controller and is registered with the Information Commissioner's Office (ICO) – Registration Number: ZA122780.

3 APPLICABLE DATA

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, for instance an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are the same as those in the Data Protection Act (DPA) 2018. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4 PRINCIPLES

In accordance with the requirements outlined in the GDPR, personal data will be:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals.

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5 ACCOUNTABILITY

Parkwood Hall Co-operative Academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The School will provide comprehensive, clear and transparent privacy notices.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records for processing activities (Data Export Record Sheet) includes the following:

a. Data ID number

b. Date of processing

c. Name and department of internal requester

d. Description of the data for export

e. Reason for the export of personal data

f. Receiving body and contact details

g. Description of technical and organisational security measures

The School will implement measures that meet the principles of data protection by design and data protection by default, such as:

a. Data minimisation.

b. Pseudonymisation (can be used as an alternative to encryption, example: Initials used to replace staff/students full names i.e. John Smith replaced by JS).

c. Transparency.

d. Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

6 DATA PROTECTION OFFICER (DPO)

The school's Governors have appointed a DPO, in order to:

a. Inform and advise the School and its employees about their obligations to comply with the GDPR and other data protection laws.

b. Monitor the School's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

c. The DPO is responsible for maintaining the Data Protection policy and associated documents. The DPO submits the policy to the Governors for review, on an annual basis.

The DPO has proficient experience and knowledge of data protection law, particularly that in relation to Schools. The DPO will report to the highest level of management at the School, which is the Chair of Governors and the Headteacher.

7 LAWFUL PROCESSING

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

a. The consent of the data subject has been obtained.

b. Compliance with a legal obligation.

c. The performance of a task carried out in the interest of the curriculum or in the exercise of official authority vested in the school.

d. For the performance of a contract with the data subject or to take steps to enter into a contract.

e. Protecting the vital interests of a data subject or another person.

f. For the purposes of legitimate interests pursued by the school as the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

a. Explicit consent of the data subject.

b. Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

c. Processing relates to personal data manifestly made public by the data subject.

Processing is necessary for:

a. Carrying out obligations under employment, social security or social protection law, or a collective agreement.

b. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

c. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

d. Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.

e. The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on a lawful basis or a contract with a health professional.

f. Reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

g. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with GDPR article 89(1).

8 CONSENT

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The School ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR. However, once acceptable consent has been obtained under the DPA, it will not be reobtained.

Consent can be withdrawn by the individual at any time.

The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child. When processing data online, parental consent is not required when the child reaches the age of 13.

9 THE RIGHT TO BE INFORMED

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the School will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

a. The identity and contact details of the school (controller), and where applicable, the controller's representative and the DPO.

b. The purpose of, and the legal basis for, processing the data.

c. The legitimate interests of the controller or third party.

d. Any recipient or categories of recipients of the personal data.

e. Details of transfers to third countries and the safeguards in place.

f. The retention period of criteria used to determine the retention period.

The existence of the data subject's rights, including the right to:

a. Withdraw consent at any time.

b. Lodge a complaint with a supervisory authority.

The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of

the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

a. Within one month of having obtained the data.

b. If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

c. If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10 THE RIGHT OF ACCESS

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data. The School will verify the identity of the person making the request before any information is supplied or viewed.

Personal data can be viewed by the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for paper copies of the information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the School holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.

11 THE RIGHT TO RECTIFICATION

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the School will inform them of the rectification where possible.

Where appropriate, the School will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the School will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12 THE RIGHT TO ERASURE

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

a. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

b. When the individual withdraws their consent.

c. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

d. The personal data was unlawfully processed.

e. The personal data is required to be erased in order to comply with a legal obligation.

f. The personal data is processed in relation to the offer of information society services to a child.

g. The School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

h. To exercise the right of freedom of expression and information.

i. To comply with a legal obligation for the performance of a public interest task or exercise of official authority.

j. For public health purposes in the public interest.

k. For archiving purposes in the public interest, scientific research, historical research or statistical purposes.

l. The exercise or defence of legal claims.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the School will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13 THE RIGHT TO RESTRICT PROCESSING

The School will restrict the processing of personal data in the following circumstances:

a. Where an individual contests the accuracy of the personal data, processing will be restricted until the School has verified the accuracy of the data.

b. Where an individual has objected to the processing and the School is considering whether their legitimate grounds override those of the individual.

c. Where processing is unlawful, and the individual opposes erasure and requests restriction instead.

d. Where the School no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, the School will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The School will inform individuals when a restriction on processing has been lifted.

14 THE RIGHT TO DATA PORTABILITY

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

a. To personal data that an individual has provided to a controller.

b. Where the processing is based on the individual's consent or for the performance of a contract.

c. When processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form.

The School will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

(School name here) is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns for more than one individual, the School will consider whether providing the information would prejudice the rights of any other individual.

The School will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the School will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15 THE RIGHT TO OBJECT

The School will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

a. Processing based on legitimate interests or the performance of a task in the public interest

b. Direct marketing.

c. Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

a. An individual's grounds for objecting must relate to his or her particular situation.

b. The School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

a. The School will stop processing personal data for direct marketing purposes as soon as an objection is received.

b. The School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

16 PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

The School will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the School has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the School's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the School to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to (School name here)'s reputation which might otherwise occur. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

a. Systematic and extensive processing activities, such as profiling.

b. Large scale processing of special categories of data or personal data

The School will ensure that all DPIAs include the following information:

a. A description of the processing operations and the purposes

b. An assessment of the necessity and proportionality of the processing in relation to the purpose

c. An outline of the risks to individuals

d. The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the School will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17 DATA BREACHES

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The DPO will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the School becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the School will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the School, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

a. The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

b. The name and contact details of the DPO

c. An explanation of the likely consequences of the personal data breach

d. A description of the proposed measures to be taken to deal with the personal data breach

e. Where appropriate, a description of the measures taken to mitigate any possible adverse effects

f. Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

18 DATA SECURITY

No personal data is to be taken offsite, unless approved by the Principal.

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access. Confidential paper records will not be left unattended or in clear view anywhere with

general access. If no longer required, paper records are to be put in to a 'white confidential waste sack' for onward secure destruction or shredded.

Hard drives and network drives are protected using New Technology File System (NTFS) permissions. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

USB Memory sticks are not be used to hold personal information unless they are password-protected and fully encrypted. Only school sanctioned encrypted memory stick can be used. All electronic devices are to be password-protected to protect the information on the device in case of theft. PC's will be read only enabled, data cannot be uploaded to USB Memory Sticks.

Dictaphones which hold confidential meeting minutes, are securely controlled by the Admin Team, the recordings are deleted after use.

The school has a remote gateway and Office 365, school staff can access school data offsite by using this secure access method. OneDrive must only be accessed via Office 365 and no data is to be saved to the users' personal device.

Staff are provided with their own secure login and password on their contract start date, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are to be password-protected and a log is maintained recording the data control.

When sending confidential information by fax, staff must always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the School premises accepts full responsibility for the security of the data. Staff are prohibited from transporting paper copies of personal data via public transport (encrypted USB sticks can be used to transport data via public transport).

School trips – For 'offsite activities student emergency information' the trip organiser is to save the information in a pdf format and upload to a Kindle device (supplied by the IT Dept). Paper copies are not to be taken offsite.

Before sharing data, all staff members will ensure:

a. They are allowed to share it (approval required from the Headteacher).

b. That adequate security is in place to protect it.

c. Who will receive it, are entitled to receive the information or are disclosed under our Privacy Notice.

d. A data sharing log is to be maintained by the Data Administrator.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the School containing sensitive information are supervised at all times.

The physical security of the School's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place. (School name here) takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Network Manager is responsible for continuity and recovery measures that are in place to ensure the security of protected digital data, which includes disabling access to electronic data when a staff member terminates their employment with the school.

19 PUBLICATION OF INFORMATION

(School name here) publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

a. Policies and procedures.

b. Reports.

c. Financial information.

Classes of information specified in the publication scheme are made available quickly and easily on request. (School name here) will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the School website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20 CCTV AND PHOTOGRAPHY

The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The School notifies all pupils, staff and visitors of the purpose for collecting CCTV images via signage. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for 30 days for security purposes; the Network Manager is responsible for keeping the records secure and allowing access.

The School will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the School wishes to use images/video footage of pupils in a publication, such as the School website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

On an annual basis the school commissions a professional photographer to take student and staff photographs for school use. The professional photographer also offers parents/guardians to purchase a photograph of their child, this is a private arrangement between the photographer and the parent/guardian.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21 DATA RETENTION AND DISPOSAL

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of the School may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. The school has adopted the HCC 'Retention Schedule for Schools', which has been created to assist schools to manage their information in line with the current legislative framework.

Paper documents are disposed of by using the provided 'crosscut' shredders (security level P-4) or the confidential waste white disposal sacks which are securely shredded by (company name here) (xxx come with a full audit trail, tracking the journey from the point of collection up until destruction). Once electronic storage devices, including photocopier hard drives are not required, they are scrubbed clean or destroyed. The Network Manager controls this process via Green Safe IT Ltd.

22 DISCLOSURE AND BARRING SERVICE (DBS) DATA

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Roles in schools are legally eligible for DBS checks and the DBS have published a 'Consent Privacy Policy' to ensure individuals are fully informed of the use of their personal data; their rights and that the school via (local authority name) meets the necessary requirements when submitting DBS checks. The 'DBS Consent Privacy Policy' explains customer rights for their data protection:

Visit: HTTPS://WWW.GOV.UK/GOVERNMENT/PUBLICATIONS/CONSENT-PRIVACY-POLICY

23 RESPONSIBILITIES

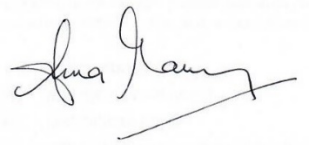
All staff within the school are responsible for protecting and ensuring the security of the personal data to which they have access and/or process. Managers and staff are responsible for ensuring that all information in their direct work area is managed appropriately, in conformance with this policy and any subsequent procedures or documents. Staff who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

The school will ensure that staff do not attempt to gain access to information that is not necessary to hold, know or process and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.

This policy does not form part of the formal contract of employment but is a condition of employment that employees will abide by. Any failures to follow the policy can therefore result in disciplinary proceedings.

APPROVAL

This Policy was written for Parkwood Hall Co-operative Academy and will be reviewed by the Finance & General Purposes Committee and approved by the Governing Body on a 2 year cycle.

Date Policy Reviewed:	28/10/2020
Date of Next Review:	28/02/2022
Signature of Governor: *(for statutory policies only)*  Date: 11/3/21	Signature of Principal:  Date: 11/3/21

Version and Date		Action/Notes
1.0	28/02/18	Creation of document.
2.0	28/10/20	Review of policy – approved F&GP 11/3/21