Aireborough Family Services

Data Protection Policy

Approved on:	22nd June 2022
Reviewed on:	17th May 2022
Next Review:	Sep 2023
Governors' Committee:	Joint Collaborative Committee
Responsible Officer:	Simon Toyne / Julia Whiteley

Contents

1. Aims

Aireborough Family Services (AFS) is committed to working effectively to provide a secure environment to protect data about staff, children, parents, visitors and other individuals that we collect, store and process in accordance with the General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for that data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

The General Data Protection Regulation (UK GDPR) is a European Directive that was brought into UK law with an updated Data Protection Act in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The UK GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The UK GDPR exists to protect individual rights in an increasingly digital world.

The UK GDPR applies to everyone, including schools. As Public Bodies schools have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the new Act and as such want to make sure information about students, parents, staff and volunteers is kept secure and within the law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data. Our governing body is the data controller. They have ultimate responsibility for how we manage data. They delegate this to data processors to act on their behalf.
Data processor	This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority. Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

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

4. The data controller

Aireborough Family Services (AFS) processes personal data relating to parents/carers and children and therefore is a data processor.

Our governing body, the **Joint Collaborative Committee (JCC)**, is ultimately responsible for how we manage data and so is registered as the data controller with the **Information Commission Officer (ICO)** and this registration will be renewed annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by Guiseley School to provide specialist services for AFS. Staff who do not comply with this policy may face disciplinary action.

5.1 **Governing board**

The governing board (JCC) has overall responsibility for ensuring that we comply with all relevant data protection obligations.

5.2 **Data protection officer (DPO)**

AFS are not required to appoint a DPO, but where required will commission the services of the DPO appointed to Guiseley School, on an adhoc basis, to assist with the development, implementation, monitoring and review of this policy .

Within AFS the **Data Compliance Officer (DCO)** is the first point of contact for individuals whose data we process, and they will liaise directly with the DPO, who is also the point of contact with the ICO.

Data Compliance Officer

Julia Whiteley
Administrator
Aireborough Family Services
Albion House
Rawdon Park
Yeadon
LS19 7XX
Julia.whiteley@aireboroughxs.co.uk

Data Protection Officer (Guiseley School)

John Walker
JA Walker Solicitor
Office 7, The Courtyard
Gaulby Lane
Stoughton
LE2 2FL
info@jawalker.co.uk

5.3 **Targeted Services Leader/Integrated Services Leader**

The TSL/ISL acts as the representative of the data controller on a day-to-day basis and delegates responsibility to the Data Compliance Officer (DCO).

5.4 The **DCO** and **TSL/ISL** will provide an annual report of their activities directly to the governing board and, where relevant, report to the board the advice and recommendations of a DPO on AFS data protection issues.

5.5 **All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their employer of any changes to their personal data, such as a change of address
- Contacting the DCO in the first instance and then the TSL/ISL if required in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our organisation must comply with.

The principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed
6. Processed in a way that ensures it is appropriately secure

This policy sets out how AFS aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 5 'lawful bases' (legal reasons) to do so under data protection law:

7.1.1 The data needs to be processed so that AFS can **fulfil a contract** with the individual, or the individual has asked AFS to take specific steps before entering into a contract

7.1.2 The data needs to be processed so that AFS can **comply with a legal obligation**

7.1.3 The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

7.1.4 The data needs to be processed for the **legitimate interests** of AFS or a third party (provided the individual's rights and freedoms are not overridden)

7.1.5 The individual (or their parent/carer when appropriate in the case of a child) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with AFS's records management procedures which follows the **Information and Records Management Society's (IRMS)** toolkit for Schools.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject Access Requests (SAR)

As an organisation we collect and process data about individuals. We explain what information we collect, and why in our Privacy Notices.

Any individual, or person with parental responsibility, or young person with sufficient capacity to make a request is entitled to ask what information is held. Copies of the information shall also be made available on request. A form to complete is available and the party making the request must provide identification evidence in order to process the request.

The information will be provided in an electronic format, within one calendar month of the request. However, in some circumstances this can be extended if the request is complicated or the data cannot be accessed. The maximum extension is up to two months.

To ensure that requests are dealt with in an effective and timely manner we may seek to clarify the terms of a request.

To collate and manage requests we have designated our DCO, to co-ordinate all requests. Please ensure that requests are made on the Subject Access request form (see Appendix V) and are submitted to the AFS office or by email to julia.whiteley@aireboroughxs.co.uk.

If staff receive a subject access request they must immediately forward it to the DCO.

Evidence of their identity, on the basis of the information set out and the signature on the identity must be cross-checked to that on the application form. Discretion about employees and persons known to AFS may be applicable but if ID evidence is not required an explanation must be provided by staff and signed and dated accordingly

Exemptions to a SAR exist and may include

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

All data subjects have the right to know:

- What information is held?
- Who holds it?
- Why is it held?
- What is the retention periods?

- That each data subject has rights. Consent can be withdrawn at any time (to some things).

They also have a right:

- To request rectification, erasure or to limit or stop processing
- To complain

Many of these questions will be within the Privacy Notice on our website.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children aged 12 and above may not be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Complaints & the Information Commissioner Office (ICO)

Our Complaints Policy, which is available from our website, deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the complaints form (see Appendix VI), and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

9.5 Other data protection rights of the individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DCO. If staff receive such a request, they must immediately forward it to the DCO.

10. Consent

As an organisation we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the UK GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

10.1 Consent and Renewal
Our 'Privacy Notice' is available on our website and explains how data is collected and used. It is important to read this notice as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for AFS. We also want to ensure the accuracy of that information.

10.2 Child consent procedure
Where processing relates to a child under 16 years old, the individual referring that child for support through our service will obtain consent from a person who has parental responsibility for the child.

Children may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

10.3 Withdrawal of Consent
Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, AFS will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate **withdrawal of consent form** for children/families (see Appendix III and Appendix IV).

11. CCTV

AFS are co-located within a Leeds City Council (LCC) rented office. LCC use CCTV in various locations to ensure its staff and those visiting the site remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DCO.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing the services of a suitably qualified DPO, when required, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where our processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of AFS, the DCO and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are required to change their passwords at regular intervals
- Where personal information in a paper format needs to be taken off site, staff must take personal responsibility for keeping that data safe
- Where personal data in an electronic format is taken off site it must be held on an encrypted laptop or encrypted pen drive.
- Staff who store personal information on their personal devices are expected to follow the same security procedures as for AFS-owned equipment (see Appendix II).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will dispose of paper-based records by placing them in the confidential waste bins within our office, which a third–party company then disposes of securely. Electronic files are overwritten or deleted. Where we use a third party to safely dispose of records on our behalf, we require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

AFS will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix I. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in our context may include, but are not limited to:

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- An email containing personal data being sent to the incorrect recipient
- Dropping or leaving documents containing personal data in a public place
- Safeguarding information being made available to an unauthorised person
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to our equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data
- The theft of a work laptop containing non-encrypted personal data about children and their families.

16. Breach notification data controller to data subject

- For every breach AFS will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.
- The breach and process will be described in clear and plain language.
- If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the DCO and DPO.
- Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.
- A post breach action plan will be put into place and reviewed.

17. Training

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or our processes make it necessary.

18. Monitoring arrangements

The DCO and TSL/ISL are responsible for monitoring and reviewing this policy.

This policy was reviewed and updated when the Data Protection Bill received royal assent and became law in May 2018 (as the Data Protection Act 2018). From then on, this policy will be reviewed **every 2 years** and shared with the full governing body.

19. Links with other policies

This data protection policy is linked to the following policies either available through the Aireborough Family Services website or on request:

- Leeds City Council's CCTV Policy
- Complaints Policy
- Privacy Notice

Appendix I: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO. The 'Data Breach Flowchart' outlines the process.

1. On finding or causing a breach, or potential breach, the staff member or data processor must **immediately** notify the Data Compliance Officer (DCO) who will then notify the Data Protection Officer (DPO).
2. The 'Data Breach form' will be completed and updated as the process progresses
3. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
   - Lost
   - Stolen
   - Destroyed
   - Altered
   - Disclosed or made available where it should not have been
   - Made available to unauthorised people
4. Evidence Collection
   4.1. It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.
   4.2. This process will be conducted by a suitable member of staff, which may be the Data Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.
   4.3. Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.
   4.4. A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.
5. The DPO will alert the DCO, the TSL/ISL and the chair of the Joint Collaborative Committe
6. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary
7. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
8. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
   - Loss of control over their data
   - Discrimination
   - Identify theft or fraud
   - Financial loss
   - Unauthorised reversal of pseudonymisation (for example, key-coding)
   - Damage to reputation
   - Loss of confidentiality
   - Any other significant economic or social disadvantage to the individual(s) concerned

   If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

9. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on our computer system (which may include one-drive for business)
10. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
      - The categories and approximate number of individuals concerned
      - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
11. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
12. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
13. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
15. Records of all breaches will be stored on our computer system (which may include one-drive for business)

Actions to minimise the impact of data breaches

The DPO, DCO and TSL/ISL will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Appendix II: Acceptable Use / Bring Your Own Device Considerations

AFS recognise that many staff choose to access information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with secured passcodes to prevent unauthorised access.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encrypted pen drives are made available to all members of staff and are available from the Data Compliance Officer.

Appendix III: Withdrawal of Consent Form (Child)

Consent Withdrawal Form – on behalf of Child

Please complete and deliver this form to the office with your signature.

Please note that we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a child, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared and the pupil is capable of expressing a view and there is conflict between the individuals the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case, a senior member of staff will discuss this with you.

Withdrawal of consent on behalf of a child

I, _____ (Parent/Carer name in BLOCK CAPITALS),

withdraw consent in respect of _____ (Child's Name in BLOCK CAPITALS)

for Aireborough Family Services to process their personal data for the purpose of _____

_____, which was previously granted.

I confirm that I am _____ (Parent/Carer name in BLOCK CAPITALS) and that I have parental responsibility for the child.

Signed: _____ Date: _____

Received by (Print name in BLOCK CAPITALS)**:**

Signature: Dated:

Actions:

Appendix IV: Withdrawal of Consent Form (Adult)

Consent Withdrawal Form – Adult

Please complete and deliver this form to the office with your signature.

Please note that we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a child, parent, staff member, volunteer or other person.

Withdrawal of consent for an Adult

I, _____ (name in BLOCK CAPITALS),

withdraw consent for Aireborough Family Services to process my personal data for the purpose of _____

_____, which was previously granted.

Signed: _____ Date: _____

Received by (Print name in BLOCK CAPITALS)**:**

Signature: Dated:

Actions:

Appendix V: Subject Access Request Form

Subject Access Request form

Data Subject (person who information is about)

Title	
Name	
Date of Birth	
School attends (if child or young person)	

Person making the request

Name	
Date of Birth	
Address	
Email Address	
Contact phone no	
Identification Evidence Provided (if required) Passport Driving licence Or two forms of Utility bill within last 3 months Bank statement of last three months Council Tax bill Rent book	

Status of person making request

Parent or person with Parental Responsibility	
Are you acting on their written authority (please provide a copy of the consent)	
If not the parent or with PR, what is your role?	

Details of Data Requested

I, ……., (name in BLOCK CAPITALS) hereby request that Aireborough Family Services provide the data requested about me.

Signature: _____ Dated: _____

I, ……., (name in BLOCK CAPITALS) hereby request that Aireborough Family

Services provide the data requested about…….. (insert child's name in BLOCK CAPITALS) on the basis of the authority that I have provided.

Signature: _____ Dated: _____

Appendix VI: Data Compliance Complaints form

Personal Details:

Name:	
Address:	
Postcode:	
Daytime telephone number:	
Evening telephone number:	
E-mail:	

If applicable, name of child(ren) and school(s) they attend:

Name	**School**

Your relationship to AFS, e.g. parent, carer, neighbour, member of the public, student:

Please give details of your complaint:

What action, if any, have you already taken to try and resolve your complaint? Who did you speak to, when and what was the response?

What actions do you feel might resolve the problem at this stage?

Signature:	
Date:	

Official Use:

Date of acknowledgment:	
By whom:	
Complaint referred to:	
Date:	