Data Protection Policy and Privacy Notice

Contents

1. Aims 2
2. Legislation and guidance 2
3. Definitions 2
4. The data controller 2
5. Data protection principles 2
6. Roles and responsibilities 3
7. Privacy/fair processing notice 4
8. Subject access requests 8
9. Parental requests to see the educational record 8
10. Storage of records 9
11. Disposal of records & equipment 9
12. Data breaches 10
13. Training 14
14. Monitoring of this policy 14
15. Links with other policies 14
Appendix 1 15
Appendix 2 16
Appendix 3 17

1. Aims

Our schools aim to ensure that all data collected about staff, learners, parents and visitors is collected, stored and processed in accordance with UK data protection 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 Data Protection Act 2018 & the UK General Data Protection Regulation (UK GDPR). UK GDPR was incorporated into UK legislation with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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

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

3. Definitions

The definitions of terms used in this policy can be found in appendix 1.

4. The data controller

Our schools process personal information relating to learners, staff, visitors, and governors and, therefore, they are data controllers. At Aspire Mrs. J Platt is our Data Protection Officer (DPO) and monitors our processing of personal information. She is the point of contact for all queries regarding data protection. Any queries should be emailed to dpo@oakfield.wigan.sch.uk or dpo@landgateschool.co.uk.

Both Oakfield and Landgate are registered as data controllers with the Information Commissioner's Office (ICO). This registration is renewed annually.

5. Data protection principles

The Data Protection Act is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully.
- Personal data shall be obtained only for specified and lawful purposes.
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed.
- Personal data shall be processed in a way that is appropriately secure.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.

6. Roles and responsibilities

The governing body has overall responsibility for ensuring that the schools comply with their obligations under the Data Protection Act alongside UK GDPR.
The schools have a legal responsibility to comply with the Act. The following responsibilities apply to the staff member(s) indicated, when investigations into data security queries are required:

Data Protection Officer (DPO)

- Liaise with the relevant Deputy Headteacher in relation to data security queries as necessary.
- Report regularly to the Executive Headteacher, relevant Head of School and Chair of Governors regarding data protection activities.
- Liaise with senior leaders on measures to prevent breaches.
- Keep required documentation in accordance with legislation and guidance available.
- Provide advice to the governing body and Senior Leadership Team as relevant, regarding school data protection queries.

Executive Headteacher

- Liaise with DPO regarding data security issues and preventative measures.
- Contribute to discussions regarding reasons for processing personal data.

Executive Business Manager

- Deputise for the DPO in their absence, covering the points listed above.
- Monitoring and evaluating data protection issues.

Deputy Headteacher

- Advise school-based staff whether or not their data security concern should be logged as a suspected breach. If clarification is needed but unable to be found, the issue should be treated as a breach.
- Liaise with the DPO regarding data security matters.
- Contribute to discussions regarding reasons for processing personal data.

Head of School

- Liaise with Deputy Headteacher/DPO regarding feedback from breach reporting, and preventative measures that should be taken in response to breaches and near misses.
- Contribute to discussions regarding reasons for processing personal data.
- Oversee queries relating to the storage, right of access to, or processing of personal data.
- Act as the representative of the data controller (school) on a day-to-day basis.

All staff

- Notify the relevant Deputy Headteacher (or if unavailable, the DPO) of any actual or suspected data breaches.
- Log any actual or suspected breaches on GDPRiS as advised by the Deputy Headteacher (or other SLT member, in their absence).

- Protect, in accordance with this policy, any personal data they collect, process and/or store.
- Notify the DPO if concerned that this policy is not being followed.
- Inform school of any changes to their personal data (e.g. change of address).
- Attend all training provided and apply learning from the training.
- Follow guidance on safe practice with data.
- Keep up to date with information shared by the DPO.

7. Privacy/fair processing notice

7.1 Learners and parents

We hold personal data about learners to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about learners from other organisations including, but not limited to, other schools, local authorities and the Department for Education. The data we hold about learners will be accessed using equipment provided by The Aspire Federation either on site or remotely (if necessary).
This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on learner characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only keep the data we collect for as long as is necessary to fulfil the purpose for it being collected.

We will not share information about learners with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of the Data Protection Policy.

Once our learners reach the age of 13 we are legally required to pass on certain information to Wigan Local Authority and other relevant support services, which have responsibilities in relation to the education or training of 13-19 year-olds. Parents, or learners if aged 16 or over (who understand data protection principles), can request that only their name, address and date of birth be passed to these organisations by informing Mrs. J Platt (DPO) or the relevant school office.

Some of our learners may complete GCSE or Level 1-2 qualifications. As part of the process to put in place the appropriate support for any written tests (e.g. extra time, reading support etc.), some learners' information may be submitted to the Joint Council for Qualifications (JCQ) for an automated decision to be made about whether the support is approved. Without sharing this information, we are unable to put support in place where it is necessary. If you do not want your data shared in this way please contact Mrs. J Platt (DPO).

We are required, by law officer, to pass certain information about learners to specified external bodies, such as our local authority and the Department for Education (DfE), so that they are able to meet their statutory obligations. We will share sensitive information with services such as occupational health, physio and speech and language therapy among others. This is so that we can look after our learners as well as possible.
In addition to sharing information to fulfil our legal obligations we will also share minimal information with companies that provide online learning tools. Information will only be shared with these companies as a way to help us to be more effective in educating our learners.

Other companies we share information with provide ways for us to track and report the progress of our learners more easily. The information shared with these companies could include sensitive information such as free school meal entitlement, ethnicity and date of birth, among other things. The reports produced by these tools for us are required by the Department for Education (DfE), Wigan Local Authority or other similar organisations.

All learners will be given the opportunity to complete qualifications. In order to do this we need to share information with awarding bodies. In turn, they will share the learners' results with us as well as the DfE. We will not share the learners' results with any other learners at Aspire or with any adults who are not staff members, unless the learner gives us consent to share their results. Ideally learners should share their results with colleges and other education providers they move onto after their time with Oakfield or Landgate. In the event that this has not happened, we will share the relevant results with them that they need to arrange appropriate education for the learner after they have left us.

As part of the Wigan outreach service we contribute to, we collect information about learners from other schools in the borough. This information is used for two reasons – the first is so that we can provide an effective service to those learners referred and the schools they are a part of. The second is to help to evaluate the impact of our service on those individuals and schools who have accessed it. This helps us to highlight areas for improvement or change.

Occasionally minimal learner information (first and surnames, and sometimes pictures) will be shared with education professionals in other schools as part of the support service we provide. This will usually be in the context of taking examples of school work to training events we deliver. The service is to help staff in other schools to improve their practice for learners with SEND by sharing our expertise in this area.

We tend to use photos and videos to document the life of the school. The photos and videos are used in line with the consent of individual learners or their parents/carers (in school, on the website, on social media or in other schools). Sometimes photos/videos of our learners, or of those who access our outreach service, are used as part of the training we provide to staff in other schools.

We are keen for our learners to be as independent as possible. As part of working towards this we provide opportunities for work experience to learners as appropriate. In this instance we will need to share some information with staff at the work experience placement to enable them to appropriately accommodate each individual learner. Information shared with the staff will not be shared with anyone else unless necessary.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The data we hold about staff will be accessed using equipment provided by The Aspire Federation either on site or remotely (if necessary). The purpose of processing this data is to assist in the running of the school, including but not limited to:

- Enabling individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body
- Provide a staff badge
- Produce documentation to distribute to learners as part of transition arrangements

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures
- Photograph (for identification purposes)

We will only retain the data we collect for as long as necessary to fulfil the purpose for which we have collected it for.

We will not share information about staff with third parties without consent unless the law allows, or requires, us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

As part of our outreach services we may, periodically, put together training resources for other schools to use. This will sometimes include videos, sometimes showing our staff. If you consent to be a part of things like these, they will be used as resources until they are deemed no longer suitable for that purpose (or until a new resource is made to update it). If a staff member who takes part in this leaves, the resource will not be deemed out of date as a result, and will still be used for as long as we deem suitable.

Any staff member wishing to see a copy of information about them that the school holds should contact Mrs. J Platt (DPO).

7.3 Visitors

We collect information about visitors who come to school in order to fulfil our safeguarding duty to our learners. Any data we hold on our network about visitors will be accessed using equipment provided by The Aspire Federation either on site or remotely (if necessary). If a visitor is to be left unsupervised in school they will need to provide evidence of a valid DBS check relating to the role they are carrying out. The signing in system will collect the following information about each visitor:

- Name
- Role
- Car registration number (optional)
- Photo
- Organisation being represented (if applicable)
- Name of person they are visiting

The system prints a badge for each visitor which should be worn at all times whilst on the premises for the purposes of identification. The information collected on the signing in system can be accessed remotely by the company providing the software (for technical assistance). In the instance that this is necessary the company has confirmed to us that the information will not be shared with anyone else.

7.4 Anyone accessing the relevant school building

CCTV may be used in and around school on corridors for the safety of our learners, staff and visitors, their property, and school property. We follow the guidance published by the ICO regarding the use of CCTV, and comply with data protection principles. The footage captured by the CCTV system will only be viewed/released in accordance with our Surveillance and CCTV policy and will be automatically overwritten periodically. Footage of specific events may be retained on disk for future reference. This footage will be released in accordance with our Surveillance and CCTV policy.

8. Subject access requests

Under the Data Protection Act and UK GDPR, learners and staff have a right to request access to information the school holds about them. This is known as a subject access request.
Subject access requests for learners must be submitted to the DPO via any member of staff, and can be verbal or in writing. Requests regarding staff information should be submitted directly to the DPO.

All requests should include:

- The learner/staff member's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

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

If a subject access request does not relate to the educational record, we will respond within 1 calendar month of us receiving the request. If the request is complicated or more than 1 request is made we will respond within 3 months. A subject access request will only be chargeable if it is repetitive or excessive.

9. Parental requests to see the educational record

Parents have the right to see their child's educational record free of charge if the child is under the age of 18. Requests for copies of some or all of a learner's educational record can be charged for. Charges are outlined in appendix 2. Requests relating to a learner's educational record will be responded to within 15 school days.
Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is deemed to be too young or unable to understand the implications of subject access rights.
For a parent to make a subject access request (see section 8), the child must give consent unless they are unable to understand their rights and the implications of making a subject access request.

Children aged 12 and above are generally seen as able to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of primary-aged learners at Aspire may be granted without the express permission of the learner. Subject access requests from parents of secondary-age (or above) learners at Aspire will usually require the express permission of the learner. These requests will be considered on an individual basis to establish whether consent should be sought from the learner.

If parents ask for extra copies of information, they may be required to pay the cost of making those extra copies.

10. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information should be kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where the room is left unlocked while unoccupied, or where visitors have/may have reason to access the room
- Passwords that are at least 8 characters long containing letters and numbers are used by staff to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- To avoid hindering learning we have not implemented complex passwords for learners to access school computers, laptops and other electronic devices

More secure password rules are in force for all users of Office 365 due to the usage of it outside of our secure networks (e.g. for remote and blended learning)

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, learners or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Remote access to the network and MIS is authorised at the discretion of the Senior Leadership of Aspire and the network/MIS **must only** be accessed while using up-to-date school-owned equipment
- Accessing the network/MIS remotely requires going through multi-factor authentication, and after a period of inactivity users will be automatically logged out. A number of failed attempts to log in results in the user being locked out

11. Disposal of records & equipment

Personal information that is no longer needed is disposed of securely. Data that has become inaccurate or out of date will also be disposed of securely unless it can, and should be, updated or rectified. For example, we will shred paper-based records and override electronic files. We also use an outside company to safely dispose of records as necessary.

Any ICT equipment that is no longer needed is sent to an external specialist company for disposal of it and any information remaining on it, in a secure manner.

12. Data breaches

A data breach can occur despite having high standards and robust procedures around data protection, particularly as information is increasingly stored online or on electronic devices. The types of breaches that can happen include the following:

12.1 Unauthorised use without damage to data

This involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

12.2 Unauthorised removal of data

This involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

12.3 Damage to physical systems

This involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

12.4 Unauthorised damage to data

This involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

12.5 Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow; or as a result of being distracted while performing a task using personal data.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data; or as a result of a successful phishing attack.
- Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

12.6 Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

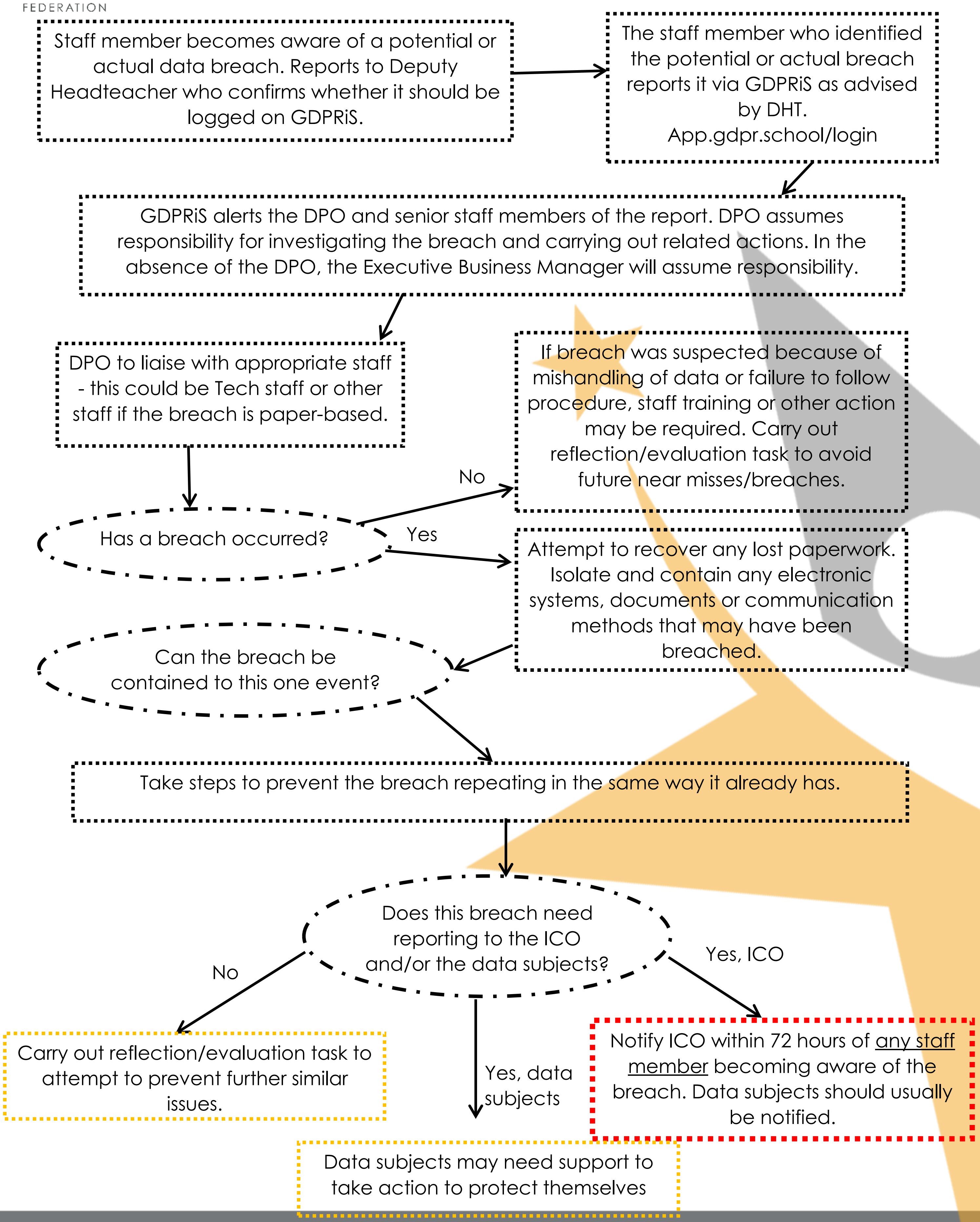
- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus or other attack.
- Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system.
- Confusion between backup copies of data, meaning the most recent data could be overwritten.

12.7 Responsibilities of the DPO in actual or suspected breaches include the following (in addition to other actions in keeping with the role of the DPO):

- Lead the investigation into suspected breaches to determine whether a breach has occurred, and any relevant actions to take in response to it.
- Document the decision and event process when dealing with all data security queries (this includes breaches, suspected breaches, near misses etc.).
- Co-ordinate all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- Assess the potential consequences, based on how serious they are, and how likely they are to happen, in order to decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis.
- Consider whether a 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). This could be through loss of control of their data, identity theft or fraud, financial loss, damage to reputation, or other circumstances that would negatively affect the data subject(s).
- Inform promptly, in writing, any data subjects who are deemed to be at risk following a data breach (see appendix 3).
- Notify relevant third parties who can help to mitigate the loss of data e.g. the police, insurers, banks, credit card companies etc.
- Notify the ICO of any data breaches that pose a negative risk to the rights and freedoms of the data subjects whose personal data is affected. This should be done within 72 hours of the breach first being suspected. Any information that is unknown at the time of reporting should be submitted as soon as possible after being received/determined.

12.8 Breaches, and potential breaches, will be managed in line with the Aspire Federation Data Breach Management Procedure. Each time a breach or a near-miss is recorded, the reflection/evaluation task will be undertaken to review and improve systems and processes to protect against future issues.

The Aspire Federation Data Breach Management Procedure



Staff member becomes aware of a potential or actual data breach. Reports to Deputy Headteacher who confirms whether it should be logged on GDPRiS.

The staff member who identified the potential or actual breach reports it via GDPRiS as advised by DHT. App.gdpr.school/login

GDPRiS alerts the DPO and senior staff members of the report. DPO assumes responsibility for investigating the breach and carrying out related actions. In the absence of the DPO, the Executive Business Manager will assume responsibility.

DPO to liaise with appropriate staff - this could be Tech staff or other staff if the breach is paper-based.

Has a breach occurred?

No

If breach was suspected because of mishandling of data or failure to follow procedure, staff training or other action may be required. Carry out reflection/evaluation task to avoid future near misses/breaches.

Yes

Attempt to recover any lost paperwork. Isolate and contain any electronic systems, documents or communication methods that may have been breached.

Can the breach be contained to this one event?

Take steps to prevent the breach repeating in the same way it already has.

Does this breach need reporting to the ICO and/or the data subjects?

No

Carry out reflection/evaluation task to attempt to prevent further similar issues.

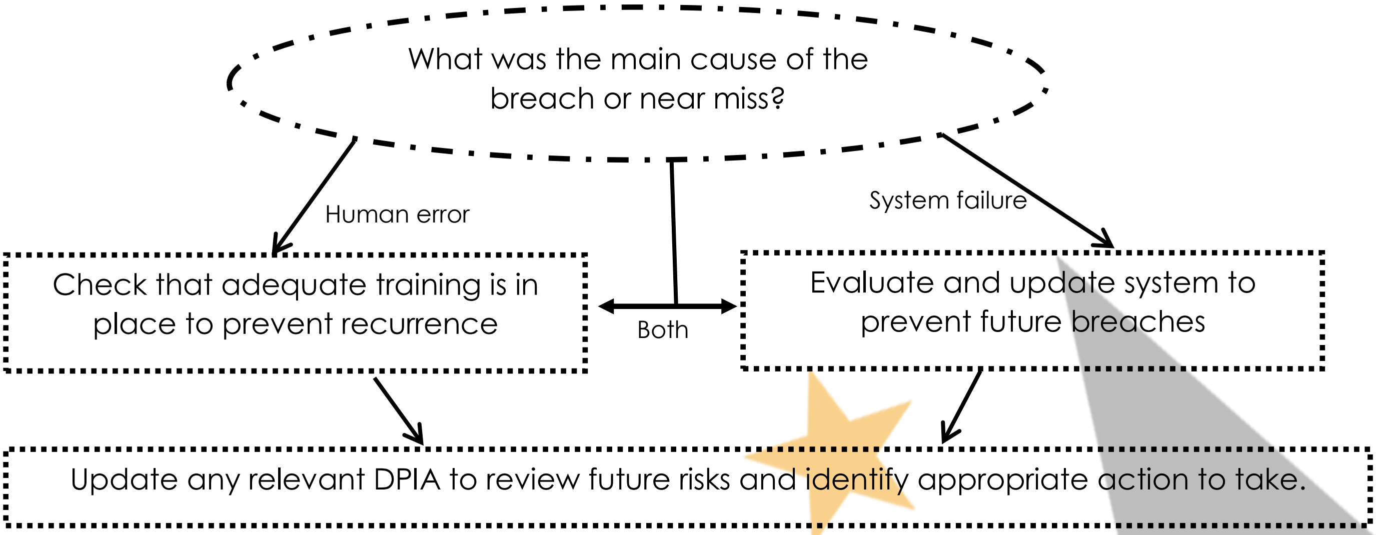
Yes, data subjects

Data subjects may need support to take action to protect themselves

Yes, ICO

Notify ICO within 72 hours of <u>any staff member</u> becoming aware of the breach. Data subjects should usually be notified.

Reflection/evaluation Task following a breach or near miss



What was the main cause of the breach or near miss?

Human error

System failure

Both

Check that adequate training is in place to prevent recurrence

Evaluate and update system to prevent future breaches

Update any relevant DPIA to review future risks and identify appropriate action to take.

13. Training

Our staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development for staff and governors, where changes to legislation or the school's processes make it necessary.

14. Monitoring of this policy

The Data Protection Officer is responsible for monitoring and reviewing this policy.

The Heads of School check that the schools comply with this policy by, among other things, reviewing school records every term.

This document will be reviewed **annually**.

15. Links with other policies

This data protection policy and privacy notice is linked to the following Aspire Federation policies:

- Freedom of Information
- Surveillance & CCTV
- Safeguarding & Child Protection
- Induction
- Social Media Policy
- Records Management & Retention Policy
- Confidential Waste Policy

Date approved:	30th November 2022
Review Date:	November 2023
Signed Executive Headteacher:	C Taylor

Appendix 1

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: Racial or ethnic origin Political opinions Religious beliefs, or beliefs of a similar nature Trade union membership Physical and mental health Sexual orientation or sex life Whether a person has committed, or is alleged to have committed, an offence Criminal convictions Biometric, where used for identification purposes
Processing	Anything done to personal data such as collecting, recording, organizing, structure, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be manual or automated.
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes and means of processing personal data
Data processor	A person, or other body, other than an employee of the data controller, who processes the data on behalf of the data controller
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data

Appendix 2

Number of pages of information to be supplied	Maximum fee (£)
1-19	1.00
20-29	2.00
30-39	3.00
40-49	4.00
50-59	5.00
60-69	6.00
70-79	7.00
80-89	8.00
90-99	9.00
100-149	10.00
150-199	15.00
200-249	20.00
250-299	25.00
300-349	30.00
350-399	35.00
400-449	40.00
450-499	45.00
500+	50.00

Appendix 3

Template notification of data breach. For people affected by the breach, deemed as being at high risk as a result of the breach.

Ref: JFP/CT

[Date]

Dear [name],

I am writing to inform you of an issue we have become aware of in relation to your/your child's personal information.

Data Protection Officer: Mrs. J Platt Email address: dpo@oakfield.wigan.sch.uk Email address: dpo@landgateschool.co.uk [delete as appropriate]	Office base: Oakfield High School & College Long Lane Hindley Green WN2 4XA
What has happened?	[Insert description of data breach incident here, including dates]
What does this mean?	[describe the possible, likely, consequences of the data breach]
What have we done about it?	[describe any measures taken (or planned) to deal with the breach and mitigate any adverse effects on the individuals concerned]

We are sorry that this has happened and we will do everything we can to make sure that the effects of this incident are minimal to you and/or your child.
If you have any questions or concerns regarding the information above, please contact me directly using the contact details above.

Yours faithfully

Mrs J Platt
Data Protection Officer