River and Lydden Primary Schools Federation

GDPR/Data Protection Policy

Date written: November 2024
Date of last update: November 2024
Date agreed and ratified by Governing Body: December 2025
Date of next full review: December 2026

	River	Lydden
Designated Safeguarding Lead (DSL)	Mrs V Alliston – headteacher@river.kent.sch.uk	Mrs C Lintott headteacher@lydden.kent.sch.uk
Deputy Designated Safeguarding Lead(s)	Ms T Moody- tmoody@river.kent.sch.uk Mrs J Brown – jbrown@river.kent.sch.uk Miss L Chase – lchase@river.kent.sch.uk Mrs S Clarke – sclarke@river.kent.sch.uk Miss C Atkins – catkins@river.kent.sch.uk	Mrs K Gibbs – senco@lydden.kent.sch.uk
Headteacher	Mrs V Alliston	Mrs C Lintott
Safeguarding Governor	Mrs E Hunt (Safeguarding lead for Governing Body) ehunt@river.kent.sch.uk	
Other key staff	Mrs J Hulks (Chair of Governors) – jhulks@river.kent.sch.uk	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals 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:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

In addition, this policy complies with regulation 5 of the Education (Pupil 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, living 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 › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › 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.

TERM	DEFINITION
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 personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
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

Each school in our federation processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Certain categories of data controller are required to pay a data processing fee to the ICO. Each school is registered as a fee payer with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mr Rob Neil from Accordio Limited and is contactable via email: **gdpr@accordio.co.uk** or telephone: 0870 490 1940

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO 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 UK
- 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 school must comply with.

The principles say that personal data must be:

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

This policy sets out how the school 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 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil 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 and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

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

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 pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed

- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

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 below the age of 12 are generally not 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 pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil'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 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with that Act.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in federations and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 2018 and the GDPR.

We will notify each parent of a pupil under the age of 18 if we wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system. We will at all times abide by the provisions for notification and parental consent as required by the Protection of Freedoms Act 2012.

We will provide reasonable alternative arrangements for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate in the collection of their biometric data. These alternative arrangements will ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result of their not participating in an automated biometric recognition system.

Likewise, such arrangements will not place any additional burden on parents whose children are not participating in such a system.

At the present time we do not, and do not intend to, collect or use children's biometric data for any purpose.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 Dawn Hunter Wardle, Business Manager.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Lydden and River Primary Schools Federation recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Lydden and River Primary Schools Federation will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

15. 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 a suitably qualified DPO, 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 data protection impact assessments where the school's 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. 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 and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable us policy)
- 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)

17. 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 shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The school 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils
-

19. Training

All 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, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- Safeguarding Policies
- Acceptable Use Policies for Staff, Volunteers and Visitors

Appendix 1a: What is a Data Protection Impact Assessment?

Introduction

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

You should ensure that you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

How should we assess a breach?

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

When do we need to notify the ICO about a data protection breach?

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So, Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, the ICO expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify the ICO of the breach when you become aware of it and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to them and tell them when you expect to submit more information.

What else do we need to do if we have a Data Protection Breach?

- ***Ensure that you inform your Data Protection Officer (DPO) immediately and follow it up with a completed Breach Notification Form so that it can be assessed and decision made as to whether it is necessary to inform the ICO about the breach.***
- ***Keep a record of any personal data breaches, regardless of whether you are required to notify them to the ICO***
- ***You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.***

How do we notify a breach to the ICO?

Your Data Protection Officer (DPO) is Accordio Ltd. In the first instance please notify us of any data breaches via email (gdpr@accordio.co.uk) and then follow it up with a completed Data Breach Notification Form once you have investigated and organised all the information.

Remember, we only have 72 hours in which to inform the ICO so it is important for this document to be completed as soon as possible.

Accordio will assess your Data Breach Notification Form and determine whether there is a need to inform the ICO of the data breach. If the assessment determines that the ICO should be informed, then Accordio will complete this on your behalf.

When do we need to tell individuals about a breach?

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform those individuals concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What happens if we fail to notify a breach to the ICO?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Appendix 1b: How to complete a Data Protection Impact Assessment

How to complete a DPIA Form

Ideally, Data Protection Impact Assessment Forms should be completed and uploaded as part of a 'New Ticket' on the Accordio Client Portal. However, they can also be emailed to gdpr@accordio.co.uk

In order to be able to fully complete the DPIA Form you will need knowledge of the project and/or system that the school/federation is considering putting in place.

You will also need to have access to or receive a copy of all GDPR Policies or Privacy Notices that have been published by the supplier (or the 'Data Processor') of the system or project if an external provider is involved. These can usually be found on supplier websites but sometimes not all the information required is detailed adequately so it may be necessary to contact them for any additional or missing information.

IDENTIFY THE NEED FOR A DPIA

- ***Detail why you have identified the need for a DPIA to be completed for this project.***
- ***Detail what the project is. If the project is to sign-up to and implement the use of an online remote learning tool or platform, please ensure that you include:***
  - ***a link to the supplier website***
  - ***Information about the system and what its benefits to the federation are***
  - ***information about the company who manages the system.***
- ***Detail what the federation is aiming to achieve and how the project will help the federation to achieve its aims, what the intended outcome will be for individuals and what the expected benefits will be for the federation, pupils, parents and for society as a whole.***

DESCRIBE THE PROCESSING

Describe the scope of the processing

NOTE: In the case of online remote learning tools and platforms this information should be detailed in the suppliers' Privacy Notice.

What data will be collected?

- The **nature** of the personal data
- ***What data will be collected and what type of data does it include***
- The **sensitivity** of the personal data
- ***Consider what personal data will need to be collected in order for the project to be successful.***

How much data will be collected and how often it will be collected?

- The **volume and variety** of the personal data
- The **extent** and **frequency** of the processing
- The **duration** of the processing
- ***The number of data subjects involved.***

Will the data be collected by an external ‘data processor’?

- ***Will the school/federation use an external ‘data processor’ to collect the data? Note: suppliers of an online remote learning tool or platform will usually be a ‘data processor’ of your federation data.***

Describe the context for the processing of this data

Consider:

- ***The nature of your relationship with the individuals***
  - How much **control** will they have?
- ***Would they expect you to use their data in this way?***
- ***Do they include children or other vulnerable groups?***
- ***Are there prior concerns over this type of processing or security flaws?***
  - What is the current state of **technology** in this area?
- ***Whether there are any current issues of public concern that you should factor in***
- ***Whether you are signed up to any approved code of conduct or certification scheme***

Describe the purposes of the processing of this data

Consider:

- ***What is the intended effect on individuals?***
- ***What are the benefits of the processing – for data subjects and your school/federation?***

Describe the nature of the processing of this data

How will the data be collected and where will it be collected from (if electronically)?

Consider:

- The **source** of the data
- ***How will the federation (or external data processor) collect and store the data?***
- ***Will there be any new technologies or novel types of processing used?***
- ***Is a third party being used to collect the data e.g. WONDE?***

Where will the data be stored?

Consider:

- ***Whether you are collecting and storing the data in your federation***
- ***Is an external 'data processor' involved with the project? Determine and detail where they will store your federation data and whether their servers are located within the EEA***
- ***Is the data is going to be stored in the US? This will be covered under the EU-US Privacy Shield***
- ***If the data is going to be stored outside of the EEA or US, where will it be stored? You will need to defer to your DPO as to whether the location is acceptable.***

How will the data be used? Will it be shared with anyone?

Consider:

- Your **relationship** with the individuals
- ***How much control individuals have over their data***
  - How likely individuals are to **expect the processing**
- ***Who has access to the data, and who the federation or external 'data processor' will share it with.***

How will the data be amended? How will you ensure it is accurate and kept up to date?

Consider:

- ***How much control individuals have over their data***
- ***Can a federation administrator amend personal data on behalf of the data subject?***

How long will data be kept for? What arrangements are there for it to be deleted?

Consider:

- ***How long you (or any 'data processor') will retain the data.***
- ***The procedures for ensuring that data is deleted***
  - Any relevant **advances in technology** or **security**
- ***What security measures you (or the 'data processor') have in place to protect the data.***

CONSULTATION PROCESS

- ***Describe when and how you will consult with relevant stakeholders and data subjects regarding the implementation of this project***
- ***Detail the need to involve anyone else from within your federation with the production of the DPIA***
- ***Consider the need to request any assistance from an external 'data processor'***
- ***Consider the need to consult information security experts or any other experts (including your DPO).***

ASSESS NECESSITY AND PROPORTIONALITY

- ***Identify the legal basis for processing this data, for example whether it is necessary to fulfil your public task of providing education, or it is necessary to be able to undertake a contract (for example with staff or suppliers).***
- ***Does the processing actually achieve your purpose?***
- ***Is there another way to achieve the same outcome?***
- ***How will you prevent function creep?***
- ***How will you ensure data quality and data minimisation?***
- ***What information will you give individuals?***
- ***How will you help to support their rights?***
- ***What measures do you take to ensure processors comply?***
- ***How do you safeguard any international transfers?***

INDENTIFY AND ASSESS RISKS

Identify any issues, risks to individuals, compliance risks and federation risks. You should consider:

- Any current **issues of public concern**
- ***inability to exercise rights (including but not limited to privacy rights)***
- ***inability to access services or opportunities***
- ***loss of control over the use of personal data***
- ***discrimination***
- ***identity theft or fraud***
- ***financial loss***
- ***reputational damage***
- ***physical harm***
- ***loss of confidentiality***
- ***re-identification of pseudonymised data***

- ***any other significant economic or social disadvantage.***

INDENTIFY MEASURES TO REDUCE RISKS

From the issues and risks identified determine whether there are any measures that can be taken to reduce the risk levels.

SIGN OFF AND RECORD OUTCOMES

Use this section to record the production, review and authorisation process of your DPIA.

Appendix 1c: Data Protection Impact Assessment (DPIA) Form

Data Protection Impact Assessment

SUBMISSION DETAILS	
PERSON COMPLETING DPIA:	
NAME OF DPO:	**ACCORDIO LTD**
SUBJECT/NAME OF DPIA	

IDENTIFY THE NEED FOR A DPIA
Explain what the project is and what the federation aims to achieve by implementing it. Summarise why you identified the need for a DPIA. You may find it helpful to refer or link to other documents, such as a project proposal.
Why have you identified the need for a DPIA for this project?
What is the project? Describe what role it plays in supporting the work of the federation. Are other organisations involved in its implementation?

What are the aims of the project?

DESCRIBE THE PROCESSING

Describe the scope of the processing: What data is going to be collected and does it include special category or criminal offence data? How much data will you be collecting and using? How often will you collect it? How many individuals are affected?

What data will be collected, and does it include special category or criminal offence data?

How much data will be collected and how often will it be collected?

Will the data be collected by an external 'data processor' in order that they can undertake their contractual obligations e.g. the federation wants to sign up to online software requiring direct access to the federations' MIS system or the federation has to provide the data via an MS Excel spreadsheet?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way?

Describe the purposes of the processing: What is the intended effect on individuals? What are the benefits of the processing – for the data subjects and your school/federation?

Describe the nature of the processing: how will you collect, use, store, amend and delete the data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

How will the data be collected / where will it be collected from (if electronically)?

Where will the data be stored?

How will the data be used? Will it be shared with anyone?

How will the data be amended? How will you ensure it is accurate and kept up to date?

How long will data be kept for? What arrangements are there for it to be deleted?

CONSULTATION PROCESS

Consider how you would consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your school/federation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

ASSESS NECESSITY AND PROPORTIONALITY

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

IDENTIFY AND ASSESS RISKS

Describe source of risk and nature of potential impact on individuals. Include associated compliance risk and school/federation risk as necessary.

IDENTIFIED RISK	**Likelihood of Harm**	**Severity of Harm**	**Overall Risk**
	Remote / Possible / Probable	Minimal / Significant / Severe	Low / Medium / High

IDENTIFY MEASURES TO REDUCE RISK

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk

IDENTIFIED	**Options to**	**Effect on risk**	**Residual risk**	**Measure approved**

RISK	reduce or eliminate risk	Eliminated / Reduced / Accepted	Low / Medium / High	Yes / No

SIGN OFF AND RECORD OUTCOMES

Item	Name/position/date	Notes
Measures approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*

Comments:		
This DPIA will kept under review by:		*The DPO should also review ongoing compliance for the DPIA*

Appendix 2a: What is a Data breach?

Introduction

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

You should ensure that you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

How should we assess a breach?

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

When do we need to notify the ICO about a data protection breach?

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So, Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, the ICO expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify the ICO of the breach when you become aware of it and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to them and tell them when you expect to submit more information.

What else do we need to do if we have a Data Protection Breach?

- ***Ensure that you inform your Data Protection Officer (DPO) immediately and follow it up with a completed Breach Notification Form so that it can be assessed and decision made as to whether it is necessary to inform the ICO about the breach.***

- ***Keep a record of any personal data breaches, regardless of whether you are required to notify them to the ICO***
- ***You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.***

How do we notify a breach to the ICO?

Your Data Protection Officer (DPO) is Accordio Ltd. In the first instance please notify us of any data breaches via email (gdpr@accordio.co.uk) and then follow it up with a completed Data Breach Notification Form once you have investigated and organised all the information.

Remember, we only have 72 hours in which to inform the ICO so it is important for this document to be completed as soon as possible.

Accordio will assess your Data Breach Notification Form and determine whether there is a need to inform the ICO of the data breach. If the assessment determines that the ICO should be informed, then Accordio will complete this on your behalf.

When do we need to tell individuals about a breach?

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform those individuals concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What happens if we fail to notify a breach to the ICO?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Appendix 2b: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- 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
- The DPO will alert the Headteacher and the chair of governors
- 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. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- 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.
- 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 the federation network, accessible only to administration staff and the federation leadership team.
- 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
- 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
- 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
- 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
- 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)
- Records of all breaches will be stored federation network, accessible only to administration staff and the federation leadership team.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the school/federation's ICT provider to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

A school/federation staff laptop containing non-encrypted sensitive personal data being stolen or hacked

- All federation staff laptops will be encrypted by default

Details of pupil premium interventions for named children being published on the school/federation website

- All pupil premium related information is double-checked before being published to ensure that personal information is not made available

Appendix 2c: How to complete a Data Protection Breach Notification Form

How to complete a Data Protection Breach Notification Form

Ideally, Data Protection Breach Notifications Forms should be completed and uploaded as part of a 'New Ticket' on the Accordio Client Portal. However they can also be emailed to gdpr@accordio.co.uk

In order to be able to fully complete the Data Protection Breach Notification Form your Data Protection Lead in federation will need to have completed a full investigation.

Outline of the Breach

Document the facts relating to the breach and its effects:

- ***Details of the breach that has occurred***
- ***Where did the breach occur***
- ***When did the breach occur***
- ***How long the breach has been happening***
- ***What effect has the breach had on the security of personal data***

Which data subjects are involved?

Are the data subject involved in the breach: pupils, staff, governors or other visitors to the school?

Data type involved?

Does the breach involve personal data? If so, what personal data?

Which member of staff reported the breach to the federation Data Protection/GDPR Lead?

Has the breach been reported to the data subjects involved?

If the breach is considered 'high risk', the data subjects should be informed of the breach as soon as possible. Please indicate whether you have done so or leave uncompleted if you require advise from Accordio, your DPO.

Has the breach been reported to your DPO?

As Accordio is your DPO please make sure that you have informed us via email if you have received notification of a data protection breach and follow it up with the completed data protection breach notification form (via the Accordio Client Portal) as soon as possible.

Actions that have been taken regarding the breach?

What effects has the breach had and what remedial action has been taken. This is part of your overall obligation to comply with the accountability principle, and allows the ICO to verify your federation's compliance with its notification duties under the GDPR.

Preventative actions that have been taken to prevent a recurrence of the breach?

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented.

Consider:

- ***Could the breach have been avoided if a better process/procedure was in place?***
- ***Is it necessary for refresher or additional staff training to be organised?***
- ***Does this involve a new member of staff who has not yet completed data protection training?***
- ***Are there any other corrective steps that could be considered?***

Appendix 2d: Data Breach Form

DATA BREACH NOTIFICATION

Date:	Person responsible for dealing with breach:				
Outline of breach					
Which data subjects are involved?					
Data type involved					
Reported by					
Phone/email sent to DPO	Y / N	Is this high risk?	Y / N	Report to ICO	Y / N
Date reported to data subjects					
Actions taken					
Preventative action suggestions – including training					

Notes		
Actions approved by		Date