Guide to data protection

September 2020

Published date: September 2020	Next review deadline: September 2021 (or sooner if required)	Non-statutory	Executive Lead at ATT: Andy Gannon Head of Corporate Affairs

Associated documents:	
• DfE data protection toolkit and checklist for schools • ICO guide to data protection • IRMS schools toolkit	
Links to:	
Policies and procedures: • Data protection policy • Privacy statements • Freedom of information policy and FOI publication scheme	

Contents

Introduction and key points for all

We take our responsibilities in the realm of data protection very seriously. This guide is intended to help and support all our people to understand the important role they play in handling personal data.

The term 'personal data' does not just refer to information held within a computer system. Nor does it just refer to things like contact details. The range of data we hold is very wide ranging, including information about learners' home circumstances or academic achievement. It can even include things that are just told to you on a daily basis, or images of individuals captured by CCTV.

Essentially, whatever you know about an individual (as long as it is specifically about an individual rather than a group of people) could be thought of as 'personal data'. It is worth remembering this.

You will also hear people talk about 'processing' personal data – this, again, does not just mean the act of inputting it to a computer system. If you are told something about a pupil and use it to redesign something you are working on with them, or if you simply pass the information on, you have technically 'processed' that data. We all do it all the time!

There are a limited amount of reasons allowed in law for organisations to 'process' personal data. In most cases, our legal justification for what we do is that it is 'in the public interest'.

The only time we should ever need to seek specific consent for the processing of personal data is if it is not directly related to carrying out the business of education. That is why, for example, you do need to seek specific and explicit consent for pupils' photographs to be published in a newsletter or online, since whether they appear or not will not have a direct impact on their education.

Having said that, though, there are three really important obligations that we must all remember in relation to personal data. We must

- **only process data which is strictly necessary for the purpose of education** (this includes safeguarding of course, and don't worry, that doesn't mean you can't talk to people about unrelated things, but you should make sure that any decisions you are making within your work are based on legitimate information) – clearly this applies most obviously to the information we record and store in our computer systems and databases
- **make absolutely sure that personal data is securely processed and stored** (this is not just about software systems but also about not leaving laptops open where they might be accessible by other people and not losing pieces of paper that have personal data on them)
- **only keep the data for as long as is required** – this is mostly an organisational responsibility and we have clear guidelines about this, but, if you have been employed by us for a while, you may wish to make sure you haven't got any twenty-year old student registers still up in your loft!

Finally, remember, too, that we all have 'personal data'. In your work you may deal with personal data not only about pupils, but also other staff and volunteers and even other companies – such as those who supply us with goods. And you have rights also about how your own data is processed by us as your employers – we have to obey the same rules in relation to that.

Which is a good note to end on – because although data protection can sound a bit scary (and there are certainly pitfalls and potentially large penalties for us as an organisation if someone gets it wrong), the majority of it is common sense. If a data protection question arises, as yourself how you would feel if it were your data being processed, and you will usually arrive at the right answer.

How we organise data protection

Everyone working or volunteering within our Trust has a personal responsibility to understand the principles of data protection and to apply them in how they do their job.

Each academy has a **data protection lead** whose role descriptor is below. On a practical level, their job is to make sure that people receive training in the area of data protection, to offer advice if needed and to take a lead in making sure the academy's procedures are all correct and responding if anything goes wrong.

We are required to have a senior member of staff who acts as our **data protection officer (DPO)**. Within our Trust, this person is Andy Gannon, Head of Corporate Affairs, and Andy supports the DPLs in each academy as well as overseeing Trust-wide policies and procedures.

All our DPLs form part of a Team Network Group which meets at least once a term so that we can further develop our understanding of, and practice in, matters relating to data protection.

Data protection lead – role descriptor

The duties of DPL within our academies are taken on by a variety of individuals, who also have other 'main' roles.

Key responsibilities and tasks:

- Act as the key contact within the academy for the Trust Data Protection Officer (DPO)
- Undertake relevant training as required or as prescribed by the Trust
- Be familiar with the requirements of the Data Protection Act and GDPR
- Be familiar with and contribute to the Trust's Data Protection policy, with other data-related policies (eg Freedom of Information, CCTV and Subject Access Requests)
- Develop an ethos and culture within school for best practice around data protection
- Regularly review data protection information, guidance and resources on academy website
- Oversee and distribute information and training in respect of data protection
- Ensure staff are regularly trained in data protection and records of this training are kept
- Ensure relevant privacy notices are issued to individuals, as necessary (staff, parents, etc.)
- Identify and monitor the data processors at work, ensuring that they deal with data in a manner consistent with data protection principles
- Monitor data management procedures within school ensuring legal compliance
- Report on data protection at an academy level to governors and the Trust
- Lead on the response to requests for information by data subjects, ensuring they are addressed within legal timeframes
- Ensure data is destroyed when necessary in line with published guidelines
- Ensure the effects of any data breaches are mitigated as swiftly as possible
- Promptly report (within 24 hours) any data breaches within school to the Trust DPO
- Assist Trust DPO with reporting data breaches to the Information Commissioner's Office
- Perform regular audits and spot-checks to ensure procedures are compliant with regulations
- Support Trust-wide compliance auditing in relation to data protection
- Undertake any other tasks related to data protection as part of the academy's and the Trust's endeavours to constantly improve practice

Responsibilities of all our people

If you have read the introduction to this document, you already have a good idea about what your responsibilities are.

Here are a few more specific things that you should think about to make sure that

- you only process personal data which is necessary
- you keep it secure
- you only keep it for as long as needed.

Electronic data security

1. Screen lock devices when you are away from them
2. Ensure personal devices (USBs/Hard drives) are secured with a pin or passcode
3. Do not share passwords or printer codes and make sure you do not use obvious passwords
4. Avoid sending personal data by email outside the Trust unless you can guarantee that the recipient is genuine and has a genuine reason for needing the data and their email system is secure – simply 'encrypting' an email does not provide this guarantee. It is often better to put the data in a document which is passworded and send the password in a separate email than it is to have the data in the body of the email itself. Ask your DPL if you are unsure.
5. Take care over emails that look like 'spoof' emails. If it looks a bit dodgy then it's probably not real. Do not click on links you receive in emails unless you are absolutely sure of where you are being taken.

Physical data security

1. Keep paper documents containing personal and/or sensitive data in a secure (locked) place.
2. If you have photographs or personal data on walls (for example for reference in an office) ensure the office or room is locked whenever you are not present. If you cannot guarantee this, then do not keep things on walls or in view in this way.
3. Do not keep personal or sensitive data in a place where it can be stolen, such as in your car. Treat personal data as you would treat your own valuable possessions.
4. Ensure you only divulge information if you are certain that the person you are talking to has a genuine reason for needing to know it.

When things go wrong

1. If you are concerned that personal data may have either gone missing or been accessed by people who should not have done so, you must tell your DPL immediately. They will be able to advise on the next steps and it is likely they will put into place the arrangements needed in the event of a data breach.

HOWEVER

Remember what we said in the introduction about common sense! Don't encrypt absolutely every email you send, just in case. Certainly for emails anywhere within our Trust, we are all bound by the same responsibilities so you should never need to encrypt emails to other staff. And if you do stop at the supermarket on the way home and remember there is a class list in your bag, then take it with you along with your shopping list!

Training for staff

It is the DPL's responsibility to make sure that training is arranged for staff as follows:

- All staff should receive a short update training session as part of a staff PD day towards the start of each year, reminding them of their responsibilities outlined above and giving them the chance to ask questions – this should also remind them of the procedures around subject access requests, the retention of data and data breaches – there are some good, free resources and videos available at https://www.gdpr.school/free-resources/, and our DPLs have developed a 'script' for this update.
- All staff and governors must undertake the 'GDPR for all' training course as part of our online 'Every' training system, and this must be logged.
- Senior leaders and DPLs must undertake the 'GDPR for managers training course as part of our online 'Every' training system, and this must be logged.
- Staff whose role specifically includes the direct processing of data (e.g. academy office staff and data administrators) should undertake additional online or face-to-face training in relation to specific roles and systems and the DPL can offer advice on this.
- DPLs themselves will undertake more detailed training as part of their TNG work. DPL training will be co-ordinated and recorded by the Head of Corporate Affairs.

Final note to all

We have a comprehensive data protection policy available on our portal and on our website. We also have privacy notices for students, parents, staff and customers, and you should familiarise yourself with these.

The DPL will ensure that appropriate privacy notices are available for all these groups.

Please familiarise yourselves with the contents of these policies and know where they are to refer to if you need them.

The rest of this document is intended for DPLs themselves, as it contains some of the more technical aspects of data protection – feel free to read on if you are not a DPL, as the more people who understand what our full range of responsibilities is, the better!

Guidance for DPLs

In the following pages, we give an outline of what the DPL in each academy is expected to either do themselves or make sure is in place. This guidance will build upon the work we undertake as part of the TNG.

Data breaches

Being alert to – and responding to – data breaches is probably the most important practical aspect of the role of DPL. Despite all of the good advice in this *Guide* and elsewhere, mistakes happen, and we must do the right things when they do.

A data breach can take many forms (all of the following have happened in the past six months!):

- A member of staff has their laptop or bag stolen and either or both contain personal data relating to pupils or learners
- Personal data is 'mixed up' when forms are being handed out to pupils or learners for checking (i.e. the wrong form is given to the wrong pupil)
- Personal data is sent elsewhere within the Trust by a secure method but never arrives
- A teacher posts a class list on the wall which displays significant amounts of personal data including addresses and exam results.

When you become aware of a breach (or a potential breach), you should do two things:

1. Immediately contact the Trust DPO (Andy Gannon or, in Andy's absence, contact Karen Robson who will be able to advise about cover arrangements) – the Trust is the 'data controller' and must take the appropriate steps – this conversation will offer advice about the second step
2. Immediately take steps to 'mitigate' the effect of the breach – for example, ensuring that user accounts on the laptop are disabled, retrieving erroneously circulated forms, seeking to trace missing parcels and arranging for them to be collected or taking down the list from the wall (using the examples above).

The DPO is likely to ask you to complete the form at **Appendix 1** as a matter of urgency. This is because we have an obligation to assess the risk related to data breaches and to report those which bear a high risk to the Information Commissioner's Office within 72 hours of the breach's being reported. The DPO will need as much information about the incident as possible in writing in order to decide whether this is required. **You do not ever have to report breaches to the ICO on behalf of an individual academy**.

The DPO will also ask you to take steps to inform those whose personal data may have been breached about what has happened. This most often takes the form of an email or phone call to parents, and **must** be done swiftly. You will need to be able to provide the name of a senior academy leader to whom parents or pupils/learners can speak if they want more information, and you should also advise them that

- the academy and the Trust are taking this seriously and doing all they can to mitigate risks, as well as working within the framework set out by the ICO
- they may use the academy's complaints procedure if they feel they wish to complain about what has happened (usually after speaking with the designated senior leader).

You must maintain an academy-based record of all data breaches.

Providing advice and ensuring training happens

The most important general function of the DPL in an academy is to make sure that training happens in accordance with the schedule described on page 6 and to offer advice to any member of our community (but primarily staff and, sometimes, pupils and parents) about matters relating to data protection.

In respect of advice, the three key areas this may cover are detailed below.

1. Advising pupils/parents and staff about the process for **subject access requests**
   All data subjects have the right to request a copy of the data held by an academy about them. This may include an entire pupil file, or it may be limited to specific aspects of what is held, such as specific CCTV images of a particular incident, or records relating to a specific subject. **Appendix 2** gives a lot more detail about the procedures to be followed in the event of a request, and the DPL should ensure they are familiar with what we need to do to comply when one occurs. The DPL should notify the Trust DPO when dealing with a SAR and ensure that the timescales for responding are adhered to.
2. Advising pupils/parents and staff about our **retention of data protocols**
   There are strict rules about how long we must keep information on file and our policy details these. They are as set out in the *IRMS Schools Toolkit* which is available at https://irms.org.uk/general/custom.asp?page=SchoolsToolkit. Very often, staff are unsure about what to keep and how long to keep it, so they should come to you for advice.
3. Advising staff and volunteers about how they can enhance their own processes and systems in order to better protect privacy and security. This is called *privacy by design* and, when we get it right, it is a sure sign that our culture around data protection is a positive one. As the knowledge of all of our DPLs becomes stronger, this advice should become second nature, and it would be great to get to a place where all our people are constantly reviewing their own working practices to ensure strong data protection is in place. Specific advice for DPLs on CCTV systems is given in **Appendix 3**.

Auditing data protection practice

DPLs should also regularly audit what is going on in our academies with regard to data protection. We will work together through the TNG to develop a model of what this might look like.

In practice, there are likely to be three elements:

1. Ongoing monitoring by the DPL on a day-to-day basis – this may include speaking with staff about their practice or checking records to ensure that they conform to the requirements
2. Case study analysis – whenever there is a data breach or a subject access request, it is good practice for the DPL to review how it was handled and think about how lessons can be learned – you may also wish to proactively delve into aspects of your data processing work on a periodic basis to check they are working as they should
3. Being part of a more formalised approach to Trust-wide monitoring – from 2020-21, we intend to develop a process of shared monitoring and learning (similar to the FAR model being used for our education directorate), with DPLs (and other Trust staff) carrying out monitoring visits to all our academies.

Record of processing activities

One of the requirements of GDPR is that you maintain a record (or inventory) of all the formal processing activities undertaken in the academy. This should be kept under review, for example, if you implement a new system or if you choose to record additional information. Remember that this is about all the data which is processed within an academy so think also about the information that teachers use to do their jobs.

A document such as the one below will suffice for this purpose but try to make it as thorough as possible. We will work on common formats as part of the TNG.

Purpose of processing	*Categories of individuals*	*Categories of personal data*	*Processes in place to minimise risk*
Pupil administration	Pupils	Name Address Phone number Parent details	Obtained through secure online system Updated through secure online system
Recording attendance	Pupils Staff	Attendance records	Secure transfer of data through electronic system from teacher
Staff administration	Staff	Name Address etc	Logged centrally by one member of staff Paper files kept in locked filing cabinet
Lesson planning	Pupils	Test scores	Logged on secure recording system Teachers trained to keep paper copies securely
Managing contracts	Suppliers	Bank details etc	All contracts and finance payments logged through secure online system

Remember that 'categories of individuals' can be 'customers' (i.e. pupils/learners and parents), staff (including volunteers such as LAC members) or external stakeholders (such as suppliers or local organisations.

Data asset register

You should also keep a simple register of the systems you use to process data, such as the one below.

Name of system	*Use and reason for data processing*	*How data stored*	*Risks*	*Retention*
Evolve	To record details about trips, including medical information about pupils	Stored and processed through Evolve, not shared more widely	All staff can access data with their password	In line with Trust policy
EntrySignIn	To record details of visitors to site, including vehicle registrations	Stored on central computer in reception	None, as only IT manager can access data	In line with Trust policy

Data protection impact assessments (DPIA)

If you implement a new system, or start a new project, you should carry out a DPIA to ensure that you do not miss any aspects of the new approach which will impact upon your data processing activities.

You must carry out a DPIA if the new activity is likely to result in a high risk to individuals. It is good practice to always carry out a DPIA, but if you decide not to, you must record the reasons why.

In practice, most DPIAs within our Trust will cover Trust-wide activities and so we can work on them together, but some more details and a template are included at **Appendix 4**.

Appendix 1 – Data breach procedure and notification form

In the event of a suspected or identified breach, we will take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring. Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible. This will be led by the Data Protection Lead for each academy.

We will also comply with our legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

Failing to appropriately deal with and report data breaches can have serious consequences for the Trust and for **data subjects** including

- identity fraud, financial loss, distress or physical harm
- reputational damage to the Trust
- fines imposed by the ICO.

Identifying a data breach

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

This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches include leaving a mobile device on a train, theft of a bag containing paper documents, destruction of the only copy of a document, sending an email or attachment to the wrong recipient, using an unauthorised email address to access personal data or leaving paper documents containing personal data in a place accessible to other people.

Reporting a data breach upon discovery

If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Data Protection Lead (DPL) for their academy immediately. The DPL will in turn immediately contact the Data Protection Officer ("the DPO"), Andy Gannon, by email to DPO@academytransformation.co.uk. The DPO will ensure that appropriate cover arrangements are in place for any periods of absence.

The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

If it is considered to be necessary to report a data breach to the ICO then we must do so within 72 hours of discovery of the breach. We may also be contractually required to notify other organisations of the breach within a period following discovery.

It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the DPL and/or the DPO immediately. Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation

The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any **personal data**. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include remote deactivation of mobile devices, shutting down IT systems, contacting individuals to whom the information has been disclosed and asking them to delete the information or recovering lost data.

Breach investigation

When we have taken appropriate steps to minimise the extent of the data breach we will commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover what data/systems were accessed, how the access occurred, how to fix vulnerabilities in the compromised processes or systems and how to address failings in controls or processes.

Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis

In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform us as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

Such an analysis must include

- the type and volume of **personal data** which was involved in the data breach
- whether any **special category personal data** was involved
- the likelihood of the **personal data** being accessed by unauthorised third parties
- the security in place in relation to the **personal data**, including whether it was encrypted
- the risks of damage or distress to the **data subject**.

A breach notification form provided by the DPO must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence in regard to any decision to report the breach to the ICO.

External communication

All external communication must be managed and overseen by the academy's DPL, liaising with the DPO.

Law enforcement

The DPL and/or DPO will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above. The DPO and/or DPL shall coordinate communications with any law enforcement agency.

Other organisations

If the data breach involves **personal data** which we process on behalf of other organisations then we may be contractually required to notify them of the data breach. We will identify as part of our investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

If we are the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then we have 72 hours to notify the ICO if the data breach is determined to be notifiable.

A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

- the type and volume of **personal data** which was involved in the data breach
- whether any **special category personal data** was involved
- the likelihood of the **personal data** being accessed by unauthorised third parties
- the security in place in relation to the **personal data**, including whether it was encrypted
- the risks of damage or distress to the **data subject**.

If a notification to the ICO is required then see part 7 of this policy below.

Other supervisory authorities

If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach.

The communication will be coordinated by the DPL and will include at least the following information:

- a description in clear and plain language of the nature of the data breach
- the name and contact details of the DPL
- the likely consequences of the data breach

- the measures taken or proposed to be taken to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

There is no legal requirement to notify any individual if any of the following conditions are met:

- appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption)
- measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise
- it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Press

The DPL must inform the DPO of any potential press interest following an actual or suspected data breach. Only the DPO can authorise any engagement with the press.

Evaluation and response

The DPL must maintain a record of all breaches within an academy, and must ensure that the volume and nature of breaches are reported to both the academy leadership team and the Local Academy Committee on a regular basis. Such reporting should focus on lessons learned.

Reporting is not the final step in relation to a data breach. We must seek to learn from any data breach.

Therefore, following any breach, the DPL must conduct an analysis as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

The DPO will maintain a Trust-wide record of breaches and report to Trustees in a similar way.

ICO Breach Notification Report

1. Organisation Details

Name of Organisation	**Academy Transformation Trust – The Nicholas Hamond Academy**
Data controller's registration number (if applicable).	
DPO	**Andy Gannon, Head of Corporate Affairs**
Contact Details	**DPO@academytransformation.co.uk** **07880 190318**

2. Details of the data protection breach

Set out the details of the breach and ensure that all mandatory (*) fields are completed.

(a) * Please describe the incident in as much detail as possible.

(b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the DPO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Details of the personal data placed at risk

Set out the details of the personal data placed at risk as a result of the breach and ensure that all mandatory (*) fields are completed.

(a) * What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the academy about the incident?

4. Containment and recovery

Set out the details of any steps the academy has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) * Has the academy taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has the academy taken to prevent a recurrence of this incident?

5. Training and guidance

Set out the details of any steps the academy has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) Does the academy provide its staff with training on the requirements of Data Protection Legislation? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) Does the academy provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

This form was completed on behalf of the academy by:

Name:.....

Role: .....

Date and Time:.....

Appendix 2 – subject access request (SAR) procedure

All data subjects have rights of access to their personal data. This document sets out the procedure to be followed in relation to any requests made for the disclosure of personal data we process.

Recognising a subject access request

As we process personal data concerning data subjects, those data subjects have the right to access that personal data under data protection law. A request to access this personal data is known as a subject access request or SAR.

A data subject is generally only entitled to access their own personal data, and not to information relating to other people.

Any request by a data subject for access to their personal data is a SAR. This includes requests received in writing, by email, and verbally.

If any member of our workforce receives a request for information they should inform the Data Protection Lead for their academy (DPL) or the Trust's Data Protection Officer (DPO) as soon as possible.

In order that we are properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally will be asked to put their request in writing.

A SAR will be considered and responded to in accordance with data protection law.

Verifying the identity of a requester

We are entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.

Where we have reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

- Current passport
- Current driving licence
- Recent utility bill with current address
- Birth/marriage certificate
- P45/P60
- Recent credit card or mortgage statement.

If we are not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of personal data resulting to a data breach.

Fee for responding to requests

We will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively, we may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable we will inform the requester, why this is considered to be the case.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

Time period for responding to SAR

We will respond to a SAR within one calendar month. This period will run from the later of

- the date of the request
- the date when any additional identification (or other) information requested is received
- payment of any required fee.

In circumstances where we are in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester the written authorisation of the data subject has been received (see below in relation to sharing information with third parties).

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, we will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

Form of response

A requester can request a response in a particular form. In particular where a request is made by electronic means then, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

Sharing information with third parties

Data subjects can ask that we share their personal data with another person such as an appointed representative (in such cases you should request written authorisation signed by the data subject confirming which of their personal data they would like you to share with the other person).

Equally if a request is made by a person seeking the personal data of a data subject, and which purports to be made on behalf of that data subject, then a response must not be provided unless and until written authorisation has been provided by the data subject. We will not approach the data subject directly but will inform the requester that we cannot respond without the written authorisation of the data subject.

If we are in any doubt or have any concerns as to providing the personal data of the data subject to the third party, then we will provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Personal data belongs to the data subject, and in the case of the personal data of a child regardless of their age the rights in relation to that personal data are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the personal data of their child.

However, there are circumstances where a parent can request the personal data of their child without requiring the consent of the child. This will depend on the maturity of the child and whether we are confident that the child can understand their rights. Generally, where a child is under 12 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their personal data on their behalf.

In relation to a child who is 12 years of age or older, then provided that we are confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, we will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child in accordance with the process above.

In all cases we will consider the particular circumstances of the case, and the above are guidelines only.

Withholding information

There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case by case basis.

Where the information sought contains the personal data of third party data subjects then we will consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information.

If this is not possible, we will consider whether the consent of those third parties can be obtained. If consent is refused, or it is not considered appropriate to seek that consent, then we will consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not, then the information may be withheld.

So far as possible, we will inform the requester of the reasons why any information has been withheld.

Where providing a copy of the information requested would involve disproportionate effort we will inform the requester, advising whether it would be possible for them to view the documents in person or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.

In certain circumstances information can be withheld from the requester, including a data subject, on the basis that it would cause serious harm to the data subject or another individual. If there are any concerns in this regard, then the DPO should be consulted.

Process for dealing with a subject access request

When a subject access request is received, you must:

- Notify the relevant DPL who will be responsible for managing the response
- Acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days
- Take all reasonable and proportionate steps to identify and disclose the data relating to the request
- Never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted
- Consider whether to seek consent from any third parties which might be identifiable from the data being disclosed
- Seek legal advice, where necessary, to determine whether we are required to comply with the request or supply the information sought
- Provide a written response, including an explanation of the types of data provided and whether and as far as possible for what reasons any data has been withheld
- Ensure that information disclosed is clear and technical terms are classified and explained.

SAR Acknowledgement Template

[On headed notepaper of data controller]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[DATE]

Dear [NAME OF DATA SUBJECT],

Acknowledgment of your data subject access request Reference: [DATA SUBJECT ACCESS REQUEST REFERENCE NUMBER]

I write to acknowledge receipt of your request for personal information which we are responding to under article 15 of the General Data Protection Regulation.

[I also acknowledge receipt of your [IDENTIFICATION] as confirmation of your identity.]

Your request was received on [DATE] and, unless there are grounds for extending the statutory deadline of one calendar month, we expect to be able to give you a response by [DATE].

The reference for your request is [REFERENCE NUMBER], please quote this on all correspondence concerning this request.

Yours sincerely,

[NAME OF SENDER]

SAR Response Template

[On headed notepaper of data controller]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[DATE]

Dear [DATA SUBJECT],

Response to your data subject access request dated [DATE OF REQUEST]

We write further to your request for details of personal data which we hold [and our acknowledgment of [DATE WHEN REQUEST FIRST ACKNOWLEDGED BY LETTER]].

We enclose all of the data to which you are entitled under the General Data Protection Regulation (GDPR), in the following format:

[DETAILS OF FORMAT IN WHICH DATA IS PROVIDED, WITH REASONS FOR CHOOSING THE FORMAT: PAPER COPIES OR ELECTRONIC COPIES ON A CD OR MEMORY STICK OR A NEW DOCUMENT WHICH HAS BEEN CREATED AND SETS OUT THE INFORMATION THAT CONSTITUTES PERSONAL DATA. WHERE THE SAR WAS MADE BY ELECTRONIC MEANS THE RESPONSE SHOULD BE PROVIDED IN A COMMONLY USED ELECTRONIC FORM.]

We enclose a copy of our Privacy Notice for your information. [ATTACH APPROPRIATE PRIVACY NOTICE].

[You will note that some of the information has been redacted. The reason for this is that the redacted information relates to [a] third part[y/ies] who have not consented to the sharing of their information with you].

[Some information has not been provided as it is covered by the following exemptions:

LIST EXEMPTIONS APPLIED]

If you are unhappy with this response, and believe we have not complied with legislation, please contact our Data Protection Officer on dpo@academytransformation.co.uk.

If you still remain dissatisfied following an internal review, you can appeal to the Information Commissioner, who oversees compliance with data protection law. You should write to: Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely,

Appendix 3 – CCTV

Our academies may use Close Circuit Television ("CCTV") within the premises.

The principles set out below apply to all members of our Workforce, visitors to the Academy premises and all other persons whose images may be captured by the CCTV system.

Purpose of CCTV

Our academies may use CCTV

- to provide a safe and secure environment for pupils, staff and visitors
- to prevent the loss of or damage to buildings and/or assets
- to assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

Siting of cameras

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. We will make all reasonable efforts to ensure that areas outside of the academy premises are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilets.

Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the academy to ensure that the proposed installation is compliant with legislation and ICO guidance.

We will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

Management and access

The CCTV system will be managed by a member of the academy leadership team, although it may be operated by other staff on a day-to-day basis. Live and recorded CCTV images will only be viewable by designated individuals and a clear justification established for the accessing of images by any other individuals.

No other individual will have the right to view or access any CCTV images unless in accordance with the guidance below regarding disclosure of images.

The CCTV system will be checked regularly to ensure that it is operating effectively.

Storage and retention of images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded, and usually not for more than 28 days.

We will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include

- CCTV recording systems being located in restricted access areas

- the CCTV system's being encrypted/password protected
- restriction of the ability to make copies to specified members of staff.

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Academy.

Disclosure of images to data subjects

Any individual recorded in any CCTV image is a data subject for the purposes of data protection legislation, and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request and this will be dealt with as such.

When such a request is made an academy leader will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The academy leader must take appropriate measures to ensure that the footage is restricted in this way. A permanent copy of such images may be provided if requested.

If the footage contains images of other individuals then we will consider whether

- the request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals
- the other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained
- it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record will be kept, and held securely, of all disclosures which sets out

- when the request was made
- the process followed in determining whether the images contained third parties
- the considerations as to whether to allow access to those images
- the individuals that were permitted to view the images and when
- whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of images to third parties

We will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with data protection legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received form a law enforcement agency for disclosure of CCTV images then academy leaders will follow the same process as above in relation to subject access requests. Detail will be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure of CCTV images then this must be complied with. However very careful consideration must be given to exactly what the Court order requires. If there

are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

Review of these guidelines and CCTV system

These guidelines will be reviewed in line with the review schedule for the Data Protection policy.

The CCTV system and the privacy impact assessment relating to it will be reviewed annually.

Misuse of CCTV systems

The misuse of CCTV system could constitute a criminal offence.

Any member of staff who misuses CCTV systems or breaches these guidelines may be subject to disciplinary action.

CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE

1 Who will be captured on CCTV?

[Pupils, staff, parents / carers, volunteers, LAC members and other visitors including members of the public etc]

2 What personal data will be processed?

[Facial Images, behaviour, sound, etc]

3 What are the purposes for operating the CCTV system? Set out the problem that you are seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

[Prevention or detection of crime etc]

4 What is the lawful basis for operating the CCTV system?

[Legal Obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime]

5 Who is/are the named person(s) responsible for the operation of the system?

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

b. siting of the cameras and why such locations were chosen;

c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

7 Set out the details of any sharing with third parties, including processors

[Police, subject access, etc. Careful consideration should be given to whether any provider is used in relation to the CCTV system and the access they might have to images. Will those processors send this data outside of the EEA, for example for storage in a cloud based system?]

8 Set out the retention period of any recordings, including why those periods have been chosen (usually not more than 28 days)

9 Set out the security measures in place to ensure that recordings are captured and stored securely

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

For example:

- Is it fair to record them in the way proposed?
- How is the amount of data processed to be minimised?
- What are the risks of the system being accessed unlawfully?
- What are the potential data breach risks?
- What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?

11 What measures are in place to address the risks identified?

12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

13 When will this privacy impact assessment be reviewed?

Approval:

This assessment was approved by the Data Protection Lead:

DPL ……

Date …….

Appendix 4 – Data protection impact assessments

You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Your DPIA must

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

If you decide not to conduct a DPIA for a new project, you must document the reasons for not doing so.

Template (from ICO)

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete 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?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
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? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to 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 organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: 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?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no

Step 7: 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 with DPIA