Data Protection Policy (including GDPR)

Policy Owner:	Sharlene Smith
Ratified by QAT Board:	June 2020
Next review date:	*This policy is currently under review as part of the Trust merger process with Q3 Academies.* *The policy details contained within the document have previously been ratified by the Board and remain in place whilst the merger review is being undertaken.*

Contents

Aims

Our Academies aim to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

Legislation and guidance

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

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

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

In addition, this policy complies with our funding agreement and articles of association.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials); • Identification number; • Location data; • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union membership; • Genetics; • 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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
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.

The Data Controller

Our Academies process personal data relating to parents, students, staff, governors, visitors and others, and therefore is a Data Controller.

The Academies are registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities

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

Local Governing Body (LGB)/QAT Board

The Local Governing Body has overall responsibility for ensuring that it's Academy complies with all relevant data protection obligations.

The QAT Board has overarching responsibility for ensuring that the LGB conforms to the obligations set out within the policies.

Data Protection Administrator/Data Protection Officer

The Data Protection Administrator (DPA) is responsible for internally auditing the implementation of this policy. They will seek advice and guidance from the designated data protection officer when required in order to ensure compliance with data protection law.

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. This provided by an external support level agreement (SLA).

The DPA and DPO will jointly provide an annual report of their activities directly to the QAT Board and, where

relevant, report to the board their advice and recommendations on Trust/Academy data protection issues.

The **DPA** is the first point of contact for individuals whose data the Trust/Academy processes, and for the ICO.

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

The DPO's responsibilities are set out in the SLA between the Trust and the external party.

Our **DPA** Lynn McIlhone, contactable via gdpr@q3academy.org.uk or at the Trust's head office (Wilderness Lane, Great Barr, Birmingham, B43 7SD. 0121 358 6186).

Our **DPO** is provided by Judicium Education services and may be contacted using the details below:

Craig Stilwell
Judicium Consulting Ltd
72 Cannon Street
London
EC4N 6AE
Tel: 0203 326 9174
Email: dataservices@judicium.com

CEO/Head of School

The CEO and Head of School jointly act as the representatives of the Data Controller on a day-to-day basis.

All staff

Staff are responsible for:

- ✓ Collecting, storing and processing any personal data in accordance with this policy;
- ✓ Informing the Trust 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 European Economic Area;
  - If there has been a data breach;
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
  - If they need help with any contracts or sharing personal data with third parties.

Data protection principles

The GDPR is based on data protection principles that our Trust 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 Trust aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- ✓ The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract;
- ✓ The data needs to be processed so that the Trust can **comply with a legal obligation**;
- ✓ The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;
- ✓ The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions;
- ✓ The data needs to be processed for the **legitimate interests** of the Trust 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 student) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. If we offer online services to students, such as Learning Room apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

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

Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's **GDPR Data Audit** and guidance set out within the Information and Records Management Society's toolkit for schools (**IRMS**).

Sharing personal data

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

- ✓ There is an issue with a student 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 students –

for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.
- We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

In all cases, personal data will only be transferred using recognised secure transfer services, such as DfE Secure Access/COLLECT, WebxChange or if this is not available, personal data will be sent within an encrypted archive or file, where the password will be sent separately. Staff are required to sign acceptance of these conditions on commencement of employment to the Trust.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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;
✓ 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.

Subject access requests must be submitted in writing, either by letter, email or fax to the **DPA**. They should include:

✓ Name of individual;
✓ Correspondence address;
✓ Contact number and email address;
✓ Details of the information requested.

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

Children and subject access requests

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

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

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;
- ✓ 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 will not disclose information if it:

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

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

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

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

Other data protection rights of the individual

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

- ✓ Withdraw their consent to processing at any time;
- ✓ Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- ✓ Prevent use of their personal data for direct marketing;

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

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

Parental requests to see the educational record

The Academy allows Parents/carers to access to their child's **educational record**. The Academy provides access to much of the data held within its MIS system on a secure "Parent Portal". Any additional access, such as that to paper files can be requested by contacting gdpr@q3academy.org.uk.

CCTV

We use CCTV in various locations around the Trust's sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV systems in use should be directed to:

Sharlene Attwood – Finance and Operations Director, Q3 Academies Trust

Photographs and videos

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials that will be used externally. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- ✓ Within our Academies on notice boards and in Trust/Academy publications, brochures, newsletters, etc.
- ✓ Outside of the Academies by external agencies such as a professional photographer, newspapers, campaigns;
- ✓ Online on our Trust/Academy websites 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. Unless consent is explicitly granted. This consent can be withdrawn at any time by contacting the **Head of School's PA**.

See our Child Protection Policy or Press Procedures for more information on our use of photographs and videos.

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 privacy impact assessments where the Trust'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;
- ✓ Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust, DPA and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

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 Learning Room desks, on Staff Lounge/Room tables, pinned to notice/display boards, 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 DAC Team (Student file), HR (for staff files);
- ✓ Passwords that are at least 6 characters long are used to access Academy computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals;
- ✓ Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- ✓ Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust owned equipment (see our ICT 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).

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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The Trust 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. Such breaches in an educational context may include, but are not limited to:

- ✓ A non-anonymised dataset being published on the Trust/Academy website which shows the exam results of students eligible for the student premium;
- ✓ Safeguarding information being made available to an unauthorised person;
- ✓ The theft of a Trust laptop containing non-encrypted personal data about students.

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 Trust's processes make it necessary.

Monitoring arrangements

The DPO and DPA are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing board.

Links with other policies

This data protection policy is linked to our:

- ✓ Freedom of Information Policy;
- ✓ ICT Policy;
- ✓ Social Networking Policy;
- ✓ Child Protection Policy;
- ✓ Recruitment and Selection Policy;
- ✓ Press Procedures & Media Policy.

Appendix 1: 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 DPA.
- ✓ The DPA will investigate the report, and after consultation with the Trust's DPO, will determine whether a breach has occurred. To decide, the DPA 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 DPA will alert the Head of School, the CEO, the Chair of the Local Governing Body and Chair of the Trust Board.
- ✓ The DPA and 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 DPA and 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); o 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 DPA and 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 "QAT Share" (L: drive) in a user-rights controlled area (i.e. only designated users can access this folder.
- ✓ 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 DPA and 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 DPA 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 DPA and 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 DPA and 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 DPA 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 in electronic format within the "Data Breach Log File", contained on the Trust network share.

- ✓ The DPA, DPO, the Head of School (and optionally, the CEO) 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 ICT department 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.*

Details of student premium interventions for named children being published on the Academy website

- ✓ *The Group IT Manager must be informed as soon as possible. The Group IT Manager or Website Administrator will then notify the DPO of the exact information released.*
- ✓ *The Website Administrator/Group IT Manager will remove the date from the Academy website immediately;*
- ✓ *The DPO will assess whether the report to the ICO and/or to inform the parents/students of those affected;*
- ✓ *The DPO will then perform an internet search to ensure that the information hasn't been trawled and is therefore accessible elsewhere. If this is the case, the DPO and the Website Administrator will contact the holding website to ensure it is removed and deleted.*

Non-anonymised student exam results or staff pay information being shared with governors

- ✓ *The Group HR Manager/Clerk to Governors should inform the DPO as soon as possible;*
- ✓ *The Clerk to Governors will then recall all paperwork sent to governors and "check in" the paperwork;*
- ✓ *If the paperwork has been released onto the QAT's governor portal, the Clerk to Governors will ensure that the information is deleted from here;*
- ✓ *The DPO will assess whether there is a need to inform parents/students/staff. In many cases, this will not be required.*

A Trust laptop containing non-encrypted sensitive personal data being stolen or hacked

- ✓ *The IT Support Department should be informed;*
- ✓ *The IT Support Department will inform the Group IT Manager;*
- ✓ *The Group IT Manager will then inform the DPO;*
- ✓ *N.B. All Academy laptops are encrypted using Bitlocker on issue;*
- ✓ *The IT Support Department will remotely disable the laptop where possible using EXO5;*
- ✓ *The IT Support Department will block email access from that device using the mechanism in Microsoft Exchange;*
- ✓ *The DPO will report the breech and inform the affected parties.*

The Academy's cashless payment provider being hacked and parents' financial details stolen

- ✓ *The Group IT Manager and DPO will be informed as soon as possible;*
- ✓ *The cashless catering payment provider (ParentPay) will close down access to all accounts whilst they investigate, updates will be provided to the DPO;*
- ✓ *The Group Finance Director, CEO and Heads of School will be informed.*
- ✓ *The DPO will inform all parents as soon as possible of the breach with advice to contact their respective banks;*
- ✓ *The DPO will inform the ICO;*
- ✓ *The Group IT Manager and the DPO will review the arrangements with the cashless provider to determine whether they are in breach of their agreement and look to the provider for advice and assurances about account information;*
- ✓ *Parents will be kept informed of the investigation by the DPO to provide assurance.*

A member of staff having a USB memory stick or hard drive stolen

- ✓ *N.B. All Academy-controlled staff devices require the user to have a Bitlocker encrypted USB device to allow them to write sensitive files to the device;*
- ✓ *IT Support should be informed immediately;*
- ✓ *IT Support "may" be able to track the usage of the missing device using Impero to allow identification of whereabouts inside the Academy;*
- ✓ *The Group IT Manager will be informed and will inform the DPO of the issue, as well as an assessment of the sensitivity of the data contained on the device;*
- ✓ *The DPO will determine whether to report to the ICO and/or affected parties.*

Unauthorised access to a member of staff's account (either remotely or on-site)

- ✓ *IT Support will be informed as soon as a member of staff is aware;*
- ✓ *The user account will be suspended whilst IT support investigate the point-of access;*
- ✓ *The Group IT Manager will be informed of the breach, informing the DPO if information has been accessed (using logs from Academy monitoring systems;*
- ✓ *If data has been accessed, the DPO will inform the ICO if the information is sensitive;*
- ✓ *On completion, IT Support will enforce a password reset and user profile reset before the member of staff is allowed access.*

Staff printing/photocopying being misplaced where personal/sensitive information is displayed

- ✓ *IT Support should be informed immediately;*
- ✓ *IT Support "may" be able to track the usage of the missing data using Equitrac/Impero to allow identification of whereabouts inside the Academy;*
- ✓ *The Group IT Manager will be informed and will inform the DPO of the issue, as well as an*

assessment of the sensitivity of the data contained on the device;

- ✓ *The DPO will determine whether to report to the ICO and/or affected parties.*

Appendix 2: GDPR and Data Protection Agreement for Staff

All Q3 Academies Trust staff are required to agree compliance with secure transfer of personal data under the circumstances highlighted within this document. A signed copy will be kept with employee contracts.

GDPR and Data Protection Agreement for Staff

GDPR – General Data Protection Regulations.

This is an enhancement to the current Data Protection legislation to increase the emphasis on the "right to be forgotten" and the responsibility that an organisation, such as a school or Academy has to ensure that the information they hold on individuals is:

a) Accurate
b) Relevant to their "business operation" or legal obligations
c) Individuals, this includes students (13 years and over) AND their parents/carers have the right to request amendments or to see their personal data that you hold
d) Secure

An Academy is classed as a "Data Controller", this means that the Academy has legal responsibility and liability for the security, control and release of all of the personal data we hold. This includes personnel, students, parents/carers and other individuals relevant to the operation of the Academy.

Personal Data is classified as:

Information that identifies an individual (directly or indirectly), such as:

e) John Smith was born on 1st January 2000
f) Dave Jones' Exam Number is X11000345
g) the Head of English's salary is £50,000

There is also a "sensitive" classification relating to areas such as:

- ✓ Racial/Ethinic
- ✓ Religious/philosophical beliefs
- ✓ Health information
- ✓ Trade-Union membership
- ✓ Sexual Orientation
- ✓ Criminal record
- ✓ LAC
- ✓ FSM
- ✓ Pupil Premium
- ✓ SEN status

ALL members of staff are responsible for the personal information they carry around with them AND what they take home. It is strongly recommended that you do not take any personal data offsite and if you do so, you should comply with the terms below.

Any loss of paperwork, sending of emails with personal information that is not protected or the loss of electronic devices, such as USB memory sticks should be reported ASAP to:

Lynn McIlhone – gdpr@q3academy.org.uk

All losses will be logged centrally, any relevant information will be collected and in certain cases, the Information Commissioner's Office (ICO) will be informed of its loss.

Therefore you, as a member of staff are responsible for:

1. Ensuring that if you do send personal information about students OR OTHER STAFF, it is encrypted. This MUST be done by either:
    a. Password protecting the Word, Excel, Powerpoint or PDF document. Instructions are available from IT Support or via the Academy website.
    b. Password protecting the collection of files within a folder using 7-zip and 256-AES encryption. Again, instructions are available from IT Support or the Academy website.
    c. Using a secure data transfer mechanism, such as S2S or WebxChange.
2. When sending emails external to the Trust, you should be sensitive to people's private email addresses. If you send ANY email to external contacts, send the message using "BCC" in order to preserve the identity of others within the email.
3. Making sure that you have collected all personal information that you release from the Academy's "Follow-Me" print system, before leaving the photocopier, particularly in areas that the students may access (FLCs, LSC, Computer Rooms, DT).
4. If you take documents home containing personal information, YOU are responsible for this. Any loss MUST be reported to gdpr@q3academy.org.uk.
5. If you copy personal information to take offsite, it MUST be encrypted using a method from point 1 or copied onto an encrypted USB Device. IT Support can advise on this.
6. Wherever possible, you should secure personal information in paper form in locked drawers or filing cabinets.
7. Reporting ANY potential breach to the Data Protection Administrator – Lynn McIlhone AND complying with any requests relating to this breach (this could be via HR, Payroll, Finance, Student Data/DAC, IT or the outsourced Data Protection Officer [DPO]).