DATA PROTECTION TRAINING OUTLINE

GDPR & DPA 2018

Data Protection laws introduced and updated in 2018 emphasis safeguarding personal and sensitive data. These include rules for aspects of how data is collected, stored, shared, used and disposed of.

Individuals also now have more control over how their personal data is processed and sensitive personal data is afforded a higher level of protection.

WHAT IS PERSONAL DATA

Personal data is any information relating to an identified, or identifiable, person whether, directly or indirectly.

This may include information such as the person's:

- Name
- Contact details (Address, Phone number, email address)
- Identification number (such as UPN)
- Online identifier, such as a username
- Date of Birth
- Salary
- Appraisal or performance management outcomes
- Examination and assessment results

WHAT IS SENSITIVE DATA

Special category data items are highly sensitive pieces of information about people. This type of data has given extra protection in terms of the reasons you need to have to access and process that information.

Sensitive or special category data includes information about a person's:

- FSM / PP Status
- SEND Status
- Looked after / In care status
- Ongoing or previous safeguarding or child protection issue
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic information
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Data relating to criminal offences is also afforded similar special protection.

THE LEGAL BASES – REASONS FOR USING PERSONAL DATA

GDPR sets out six legal bases (reasons) for processing personal data. At least one of these must apply whenever you process personal data:

1. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

2. **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests**: the processing is necessary to protect someone's life.
5. **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

FCAT's Privacy Notices outline which of these legal bases we rely on for processing personal data.

There are some exemptions defined in the Data Protection Act 2018.

[Discuss examples of each basis]

WHICH BASES WE RELY ON

We only collect and use personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest
- We need to fulfil a contractual obligation

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

CONSENT

There will be times when consent is required to process personal data. This will most commonly be when and where pupil's photographs are used and shared.

GDPR sets a high standard for consent.

Explicit consent requires a very clear and specific statement of consent.

Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.

Requests must be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.

When asking for consent you must also include a statement informing individuals that consent can be withdrawn at any time. Include with details of who to contact and how to contact them.

[Show FCAT photo consent form]

EXEMPTIONS

The Data Protection Act 2018 sets out exemptions from the GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within the GDPR do not apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption is the one related to requests from the police for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching the GDPR or Data Protection Act 2018.

This does not mean we must comply with every request from the police. Before information is shared with the police under this exemption the police must make the request for personal data using a DP1 form. This is an official police document which specifically outlines the personal data requested, the reason for the requested personal data including if it related to the prevention or detection of crime or the apprehension or prosecution of offenders.

Once a DP1 form has been received it is still up to the data controller (academy) to decide whether it would be in the best interest of the relevant parties for the information to be disclosed.

[Show DP1 Form]

HOW DOES THIS AFFECT FCAT?

We [FCAT] must:

- ensure that we only collect and use personal data for specific and justified purposes
- be transparent about the data we collect, share and use personal and sensitive data. We do this through Privacy Notices issued to students, parents and staff
- be constantly thinking about the reasons we collect, share and use personal and sensitive data
- keep detailed records of the data we hold, who we share it with and how we keep it safe
- report any suspected data breach to ICO within 72 hours

TRANSPARENCY / PRIVACY NOTICES

- The personal data we hold
- Why we use the data
- Our legal bases for using the data
- How we collect the data
- How we store the data
- Who we share the data with
- Individuals rights regarding personal data

EMPLOYEE EXPECTATIONS AND RESPONSIBILITIES

All staff are responsible for safeguarding personal information and must ensure that personal data is processed for specific and justified purposes.

- You must always be careful and thoughtful when working with information that could be used to identify or be linked to a pupil, parent or member of staff
- You must consider whether you need personal data to achieve your objective
- You must only process the minimum amount of personal data required to perform a task
- You must do everything you can to safeguard the personal data that you access and use. Use common sense, especially when handling sensitive personal data such as pupil premium status and medical conditions. Think carefully about who actually needs to know this information and where you hold any conversations to ensure no one can overhear
- You must only disclose personal data when you have an individual's consent to do so or where there is another legal basis for doing so.
- You must ensure you verify the identity and contact details of a contact before you disclose the personal data
- You must report a suspected data breach to the Principal and DPO within 48 hours

[Refer to the Data Protection Employee Responsibilities Document]

EMAIL

Emails present a significant amount of risk where data protection is concerned. Accidentally sending an email and/or attachment containing personal data to the wrong person can easily occur.

- Wherever possible emailing of personal or sensitive data should be avoided, if it is necessary to share personal data consider if this could be done using Google Drive
- If emailed, any sensitive data must be attached using a password protected **and** encrypted document, the password must not be included in the original email but should be separately sent or use a password that is already known to the recipients
- Personal data must not be used in the subject of the email, e.g. John Smith Allegation
- File names attached to emails must not contain personal data, e.g. JohnSmithExclusion.doc
- Double check the recipient list before sending any email containing personal data
- Do not forward email chains without checking the entire content for personal or sensitive information

DATA SHARING

When we want to share personal data with a third party we must ensure that there is a data sharing agreement in place. This usually forms part of the signup process for new software and services, but we also need to have data sharing agreement in place with outside agencies such as education providers and health service professionals.

Data sharing agreements should define the "*what, why, how and when"* personal data is being shared. Details of security measures and breach reporting procedures could also be included.

If you are considering using any service, app or software that requires the use of personal data such as pupils' name you must check with FCAT's Network Manager or the DPO that appropriate security measures and agreements are in place.

DATA RETENTION AND MINIMISATION

We should ensure that we do not keep personal data for longer than is necessary. GDPR includes states *"personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)".*

There are no defined measures for how long personal data should be retained. You must be able to justify your reasons for retaining and processing personal data.

An example of this could be pupil attainment, attendance and behaviour data from a cohort of pupils who have left school.

You might want to keep this data for review purposes. Which pupils attended intervention classes and how did they affect their Key Stage 4 outcomes? Did pupils with low attendance or poor behaviour under achievement at Key Stage 4?

You might want to keep this data for benchmarking purposes, to compare current cohort data against previous cohort data.

At what point do you think it is no longer necessary to keep pupils names linked to the data?

When should this data be "blurred", "anonymised" or "minimised"?

Can the data be useful without personal data?

After a year or two you can keep the data as aggregated data, such as:

- Data for all pupils in 2017
- Data for all boys in 2017
- Data for all girls in 2017
- Data for all PP pupils in 2017

WHAT IS A DATA BREACH

We handle and process large amounts of personal and sensitive data on a daily basis, mainly related to pupils but also parents, carers, family members and FCAT employees.

A data breach occurs when someone personal or sensitive data is disclosed to, sent to or accessed by someone who does not have permission to access the data. Loss or theft of personal data is also classed as a data breach.

- Examples of a data breach include but are not limited to:
- Losing a portable media device such as a USB memory stick or external hard drive which contains personal information.
- Emailing an attachment containing pupil data to the wrong person
- Losing paper copies of your class marksheets or register, especially any those which show PP or SEN status
- Suspecting someone has gained unauthorised access to a computer system such as SIMS
- Uploading personal or sensitive information to a website, social media platform or publicly accessible cloud storage
- Disclosing personal and sensitive information over the phone to an unknown person or someone who does not have permission to access that information

[Discuss examples of recent data breaches within the Trust]

REPORTING A DATA BREACH

When a personal data breach has been discovered, it must be reported to DPO immediately.

The DPO and Principal will determine whether the breach should be reported to the ICO.

If necessary, the breach must be reported to the ICO within 72 hours.

[Show data breach reporting procedure]

[Show ICO breach reporting form]

RIGHT OF ACCESS - SUBJECT ACCESS REQUESTS

Individuals have the right to access their personal data. This is commonly referred to as subject access.

Individuals can make a subject access request verbally or in writing. We have one month to respond to a request.

Individuals have the right to know if the personal data is being process and if so they have the right to obtain a copy of the personal data we hold related to them.

An individual is only entitled to their own personal data, and not to information relating to other people (unless they are acting on behalf of someone, such as a request for pupil's personal data from someone with parental responsibility)

RIGHT OF ACCESS - PUPIL RECORDS

Pupils have a right to access the educational record.

Parents and carers also have a right to access their child's educational record.

There are certain circumstances where the school can withhold an educational record; for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual.

A request for an educational record must receive a response within 15 school days.

FREEDOM OF INFORMATION REQUESTS

The Freedom of Information Act 2000 provides public access to information held by public authorities.

It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

There are circumstances when we can refuse a request for information. We can refuse an entire request if:

- It would cost too much (£450) or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

There is also an exemption for personal data if releasing it would be contrary to the GDPR or the Data Protection Act 2018.

If we receive a request for information that includes someone else's personal data, we need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation.

We will decide whether we can release the information without infringing the GDPR data protection principles.

There maybe be circumstances where we receive a request for information and decide to both disclose some of the information and refuse to disclose some of the information.

If we decide to refuse a Freedom of Information request we must respond by issuing a refusal notice which clearly explains our decision and details which of the exemption rule(s) we have applied.

Not all Freedom of Information requests will require personal data to be disclosed.

[Discuss examples of when information has been disclosed following a FOI request]

[Discuss examples of when FOI request have been refused]