# Confidentiality/GDPR Policy

## Statement of Principle

The General Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure of personal data.

Impact Barnet is dedicated to ensuring the security of all information that it holds and implements correct procedures to ensure this whether held digitally or printed material.

To achieve this Impact Barnet will endeavour to -

- Protect against potential breaches of confidentiality.
- Ensure that all information assets and IT facilities are protected against damage loss or misuse.
- Ensuring that all members of The Impact Barnet Team (employees, volunteers, trustees, others are aware of this policy as part of any induction and ongoing training and undertaking procedures to comply with all legislation in UK law.
- Increase awareness and understanding that is the individual's responsibility to protect the confidentiality of all students, colleagues and third-party organisations.

## Physical security

- All records held in filing cabinets should be securely locked at the end of each session and any documents returned after being removed for meetings etc.
- Only designated people can have access to files when needed.
- Annual assessment to be undertaken to ensure the correct level of security.
- Care should be taken when discussing sensitive information in a public place, school corridor etc.
- All documents containing information should be carried in secure bags, cases or folders.
- Information should not be left unattended in places of risk (e.g., boots in cars, cafes etc).

## Data security

- Impact Barnet laptops should be used if possible.
- If own equipment is used, including desktop, laptops or mobile devices, these should all have an agreed level of security and encrypted access. This would also include data storage.

## Data security (cont'd)

- Emails should only be sent using an Impact Barnet email address if sending confidential data especially regarding students/schools etc.
- Distribution of information – Care should be taken when circulating especially by email those addresses are checked prior to sending.
- When Texting (SMS) to either parents/carers, students and possible other third parties this should only be done through an issued Impact Barnet Sim card and or phone.

## How and what do we communicate to parents/carers

- When there is a need to obtain parental/carers consent ensure that this is asked for in writing.
- Even if parental consent is given, it does not mean a parent/carer has the right to know the contents of the service's work with their child: they are entitled to expect the same level of confidentiality as those able to consent independently. (NB Schools would get permission for 12-16 years young people.)
- Impact Barnet must make it clear and define on what basis information will be shared with parents/carers on an individual case by case basis.

## What information can Impact Barnet pass on to other agencies?

- The process for obtaining young people's consent for specific information should ideally be in writing or written consent. The only exception to this is where members of the Impact Barnet Team deem there is a serious risk of harm and child protection procedures to be implemented.
- Ensure any proposal to share information on behalf of a young person is necessary e.g., it supports an agreed referral to another agency or is needed to protect a young person.
- Impact Barnet will set out when and how permission is actively sought from young people to share information and in what manner in which specific information is passed on.
- Impact Barnet should clearly state any evidence required to assure itself that when another agency/individual requests information about a young person, this is what the young person has consented to.
- Include the requirement for written information sharing and referral protocols with agencies with which Impact Barnet have cross – referral relationships. Make clear the position on confidentiality and the circumstances in which Impact Barnet shares information.

## Reporting Data Breaches

- All concerns of a data breach should be highlighted to team members/ trustees without delay.
- A plan of action will be drawn up to rectify the breach and a written record made of the breach with any pertinent points and actions.
- If appropriate, breach should be reported to the Information Commissioner's Office (details on GOV.uk).

## Reviewed

The policy is reviewed annually.