From: [redacted]
Sent: 11 December 2019 11:44
To: [redacted]

Subject: The Data Protection Act 2018 / the General Data Protection Regulation (GDPR)

The Data Protection Act 2018 / the General Data Protection Regulation (GDPR)

- The Data Protection Act 2018 repealed and replaced the UK's data protection laws to keep them up to date for the digital age and set new standards for protecting personal data, in accordance with the General Data Protection Regulation.
- GDPR applies to **everyone** within the OFPCC. It applies to 'personal data' which means any information relating to an identifiable person who can be directly or indirectly identified.
- This includes things like names, addresses, identification numbers, location data or online identifier (reflecting changes in technology and the way organisations collect information about people).
- It is essential that all the data we collect and hold has a **lawful basis for processing** and is kept secure.
- It is also important we only keep data for as long as we need it to undertake the work of the office. This includes, for example items such as emails, correspondence, consultation responses and financial records. There is a corporate **Record Retention Policy** which covers much of the work of the office and it is important all colleagues are aware of their responsibilities in relation to this. A copy of the policy can be found here.

- **Should there be a data breach you must report it immediately** using our online form which can be found here and make the Monitoring Officer aware of the situation and what steps you may have taken in response.
- **Non-compliance with GDPR can lead to a fine of up to €9,000,000 or approximately £8.5m for the OPFCC.** This underlines the importance of processing data correctly and securely. Therefore **it is important that we all take this seriously as leaving documents on our desks or leaving a computer unlocked could lead to a serious data breach**. This could undermine the work of the Commission, lead to catastrophic reputational damage as well as a large fine.

Individuals Rights

As GDPR gives individuals a number of rights over their personal data, **we need to ensure we record and review what information we hold.**
Individuals now have –

- The right to access
- The right to be forgotten
- The right to data portability
- The right to be informed
- The right to have information corrected
- The right to restrict processing
- The right to object
- The right to be notified

As a result of this, **we need to understand and identify what 'personal data' we hold as well it will be used, how long we will need to keep it and if it will be shared.** This will be recorded on the OFPCC GDPR Data Mapping Spreadsheet.
If personal data can be truly anonymised then the anonymised data is not subject to the GDPR.
Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
Information about companies or public authorities is not personal data.

Lawful bases for processing data

As an organisation, we need to be aware of the lawful basis for processing data. At least one of these must apply whenever we process personal data:

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

b) **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.

c) **Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).**

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **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.

The OFPCC mainly processes data where people have given us their consent and where we have a legal obligation to do so. There may be occasions where this may not be the case, if in doubt ask the Governance Team for guidance.

Special category data

Under GDPR there is also *'special category data'* which is **personal data but is more sensitive** and so needs more protection. In order to lawfully process special category data, we must identify both a lawful basis under Article 9 of the GDPR. For us it would be Article 9 (2) a – *'The data subject has given explicit consent to the processing of those personal data for one more specified purposes'.*
Special category data includes for example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Recording Data Processing

Under GDPR, **we need to maintain a record of processing activities**. This is undertaken through a GDPR Data Mapping Spreadsheet.

This should contain all the following information:

- The purposes of why we are processing the data.
- A description of the categories of data subjects and of the categories of personal data.
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.
- Where possible, the envisaged time limits for erasure of the different categories of data.

All teams must keep under constant review what personal data they currently hold, why it is held, who you share it with, how secure it is, and whether you need to keep it.
This document will be maintained by the Governance team and will be circulated to all Directors on a monthly basis for review.

Data Breaches

Any data breach MUST be reported within 72 hours to the ICO. The OPFCC has an online form to report any breach which will then go to the Chief Executive and the Data Protection Officer to consider what action needs to be taken. For example, a breach within the 'policing family' could be effectively

dealt with without a referral to the ICO. However it is vital that it is still reported and all actions are recorded. However **any breach to an outside organisation or individual must be reported.**

Non-compliance can lead to fines of up to 20,000,000 euros or 4% of annual turnover. However, for the Public Sector that figure reduces to €9,000,000 or **approximately £8.5m**.

Most data breaches occur due to human error or poor data security, therefore as an organisation it is important for everyone to keep under review manual and electronic files, folders, drawers, cabinets, walls, emails, notebooks, etc to ensure that we are not holding or displaying personal data in breach of the Data Protection Act 2018.

The simple act of leaving your screen unlocked could lead to the OPCC being in breach of the GDPR and could lead to a mandatory referral to the ICO and in the worst case scenario take over £8m from frontline policing.