SUGGESTED ANNUAL TRAINING BRIEFS

2020-2021

Contents

Version	Author	Approval Date	Publication Date	Major Review Date
V1.0	i-West	October 2020	October 2020	October 2021

INTRODUCTION

This is a suggested plan that your organisation may choose to use to for this year. It includes a series of 5-10 minute briefs that can be used as part of training sessions, general meetings, team meetings or any other scenario that may present itself as suitable for such information to be disseminated.

They are not designed to be lengthy but simple reminders of good practice to avoid commonly seen mistakes that lead to data breaches.

Included in the following sections are 14 briefs that are aimed to be used on a monthly basis, however they may be used in whatever way your organisation sees fit.

The following topics are covered;

1. Email Security
2. Clear Desks
3. Recognising Personal Data
4. Data Breaches
5. Sharing Data
6. Confidentiality
7. Disposing of Confidential Waste
8. Data Protection Rights
9. The Right of Access (Subject Access Requests)
10. Consent
11. Data Minimisation
12. Data Protection by Design

To support this learning the ICO video below will help give practical examples of the application of this guidance.

https://www.youtube.com/watch?v=ksEMs8s8En0

1. Email Security

The most common cause of specific data breaches is as a result of emails being sent to the wrong recipient. The difficulty with avoiding this type of breach is that the only methods reduce the ease and efficiency of the use of emails, so the best method for avoiding this is for individuals to be aware and mindful when sending emails to remember the following steps;

- Stop
- Think
- Check
- Send

So before hitting the send button;

STOP for a second, take a look at the address bar and the people you expect to receive this information;

THINK about whether it matches up with the content or the intention of the email;

CHECK the addresses that you have used, is it one that you have typed in directly? Then there may be a typo. Does it need to be Bcc'd? Would these people expect to know the other people's email addresses? What attachments are there?

SEND in the confidence that it is going where it should.

The use of Blind Carbon Copy (Bcc) should be used whenever contacting multiple external recipients when the message is intended to be received on an individual level.

So, ask yourself the question when you **THINK** 'is this message part of a group discussion, or am I copying everyone in to make it easier than sending it individually?' For example, a notification about an upcoming event will very likely be Bcc'd whereas an email to a number of people in another organisation, a supplier for example is unlikely to need to be Bcc'd.

Another common error is attaching the wrong file to an email or using an incorrectly named file. It is worth opening the document that you intend to attach before sending it, in some cases this may not be a significant issue, however safeguarding notes, confidential documents, and any situations where you may be sending lists of names or some form of personal data should be checked.

Stop!

THINK

and

CHECK

Send

2. Clear Desks

Ideally every piece of information will have a safe and secure place to go, however it is well known that some things will always need to be on hand. What a clear desk routine aims for is making sure that information can be found easily when it's needed, is out of sight of people who have no need to see certain things and doesn't go missing leading to a data breach.

Some simple steps to achieving a clear desk are as follows;

- If a record is highly sensitive and in a physical format, a safeguarding report, HR details, or financial details for example, you should try to return it as soon as you have finished with it, avoid piling up things to put away later.
- Keep information that is not sensitive but may be personal in a folder that can be put away at the end of the day will avoid it getting mixed up with other records.
- Use electronic records wherever possible, for example contact numbers for clients or parents may be more easily stored in a simple electronic management system or spreadsheet.
- At the end of the day make a last check to see if anything has been left out and store it away, this includes not only paper records but USB sticks, optical disks, SD cards and other devices.
- However, don't fall into the trap of creating a clutter drawer! If somethings needs to be destroyed place it in the confidential waste bin, or if a device has a secure storage location take it there.

By adopting a clear desk, the risk of breaches can be reduced, it is quite unlikely that someone will steal the information, however it is far more likely that something will be inadvertently picked up and put somewhere that the regular user is unfamiliar with or accidently destroyed.

Even if you have a specific desk and leaving all of the records out makes sense to you because you will need to carry on with it the following day the convenience of doing so is not the point. If you do share a desk it is all the more important to make sure that you keep your workspace in order to avoid a data breach.

Although a clear desk routine suggests just the desk that you may work at, take into account the surrounding environment. Have telephone numbers been attached to the wall, or passwords stuck on computer screens? Is there a better way to store these?

Some information will need to be accessible and some doesn't need to be put away, staff extension numbers for example, or reference guides etc. However, do you have the details of people's medical conditions in plain view? Although this may be important to be able to quickly reference can it be better stored in an emergency folder or incident book for example.

If you are uncertain about what sort of security is needed for some of the information that you use, you should raise the question with the Data Protection Officer.

3. Recognising Personal Data

We often think of personal data as the name, address, or telephone number of a person however the definition is far more complex.

However, the General Data Protection Regulations (GDPR) defines it as any information relating to an identified or identifiable natural person, also known as a data subject. A natural person basically means anyone who isn't deceased or a business entity. The Information Commissioner's Office, the ICO, who regulates data protection in the UK explains it further, but the key point is that it must 'relate' to someone.

What does relate mean? Well on its own nothing is really personal data, so a name for example may relate to dozens, hundreds, or thousands of people, and even with a location it may not be personal data. i.e. Olivia Harris from London could relate to hundreds of people, Olivia Harris from Westminster in London may reduce that number to a few at which point it may start to look like personal data, however, can it be related to a person yet? It is unlikely, if we add a place of work, then we can safely say that combined this constitutes personal data.

So, what does that mean for your organisation? Well the data that you capture will be from people related to your organisation, a client, an employee, a student etc which will mean that almost all data that you hold will quite easily lead to a person being identified. For example, you may hold a list of the Pupils whose parents attendees a school event, you may think that the data only identifies the pupils but in fact it will also relate to the parents as their children's names are on there and it gives a time and location, so it is in fact also the parents' personal data.

Once you take into account other pieces of information and they combine a person may be able to indirectly identify an individual. That makes it very important to consider just how much, albeit seemingly innocuous data, is disclosed.

Personal data also has two different levels, there is simple personal data, names, addresses etc and then there is something called special categories of personal data, these include such things as medical information, political or religious opinions, ethnicity information, trade union membership and sexual information. These special categories require additional safeguards and security to be put in place and they will also need a separate legal basis. Those separate legal bases are similar but are covered under a separate part of the GDPR.

If you are in doubt about what you can collect or how you should collect it you must talk it through with the data protection lead or Data Protection Officer (DPO).

4. Data Breaches

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 it can happen due to;

- Deleting records (accidental destruction)
- Malicious deletion of files (unlawful destruction)
- Losing student records (loss)
- Overwriting records by accidental (alteration)
- Sharing personal information without identifying legal basis for sharing (unauthorised disclosure) – this is one of the most common sources of breaches
- leaving confidential information on a photocopier which is then read by someone who has no reason to have access to it

The internal School Data Protection Lead must be notified of the breach as soon as possible. The person who discovers the breach might be confident enough to complete an incident form or they can work with the data protection lead to complete it but it should include the details of the incident, a brief narrative, actions that have been taken and actions that need to be taken. The relevant manager or person responsible for the data should be notified if they are not already aware as they may be able to assist.

The School data protection lead should notify the Data Protection Officer (One West) and if necessary liaise with the DPO and they will be able to guide them through the steps of dealing with the breach.

If a breach meets the relevant threshold for reporting, it must be reported to the ICO within 72 hours, this is as a result of assessment and discussion with senior staff and One West and should not done by individual staff.

In discussion with the DPO assess who has been affected and the likely risk and consequences to them and identify appropriate measures to mitigate this risk, in some cases you will need to notify the person or persons whose data has been compromised.

You can recover information that was erroneously sent from the unintended recipient by asking them to return it to you or ask them to confirm deletion.

If data has accidentally been overwritten or deleted IT may be able to isolate the source of the loss of data, this may be a computer, a mailing system or website, then re-establishing systems to normal operations, or possibly restore from backup. Remember to include all relevant people and teams who can help in secure a data breach when you are containing it or recovering data.

If a data breach happens as a result of a cyber security incident you may need to change access codes, notifying IT security [details] to implement a technical solution e.g. isolating a compromised section of the network or remotely wiping a mobile device.

You may also need to inform the police and other enforcement bodies where appropriate e.g. ransomware, theft of laptop.

After a data breach or even a near miss a review of existing controls to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

5. Sharing Data

Before any data can be processed including being shared, you need to ensure that there is a lawful basis upon which to share it. There are 6 lawful bases, which include:

- Consent, which is freely, clearly, and unambiguously given (e.g. consent to having a photo taken as recording on the annual form which is sent to students / parents)
- Legal obligation i.e. the law requires you to do something – e.g. notify the Local Authority or police in some circumstances about **safeguarding issues**
- Public task (for example delivering an education).

When you wish to share / process special category personal data (such as health, special needs, disability) you need to satisfy an additional condition for example:

- Explicit consent to sharing the personal data for example the health information
- For employment purposes
- Public health (for example sharing test and trace information)
- Vital interests (life or death situations eg with an ambulance crew)
- Legal claims (eg if the school was defending a personal injury claim)
- Substantial public interest (the situations that qualify are set out in a prescribed list and include safeguarding)

Choosing the correct basis for sharing can be complicated and we would recommend that you consult your data protection lead to discuss. When discussing data sharing as part of **safeguarding** everyone should read: Information Sharing Advice for Practitioners which is a DfE publication and refers to the 7 Golden rules of information sharing. These rules are as follows;

1. The GDPR and Data Protection Act 2018 are not barriers to justified information sharing.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

6. Confidentiality

Confidentiality means keeping data, which is private, personal, or sensitive in relation to the person who gave it to you secure from being shared or accessed by anyone who shouldn't have access to it. the word can be used more or less interchangeably with security but there are subtle differences.

An example would be when a student shares a concern with you about another student or teacher and how you then go about acting on that information. We spoke previously about legal basis for sharing but in the case of confidentiality it may be that even though there is a legal basis it would be unethical or poor judgement to share that information. Imagine telling someone a personal secret and that person then telling others, there's no law that says that it can't be shared but it is an ethical question.

These ethical questions arise particularly around concerns raised in the area of safeguarding, a person may tell you something about a child but it may not be appropriate to directly discuss the matter with the parents of the child but in fact to have a confidential discussion directly with the child, in that example any information that the child provides would be confidential.

In a school setting information may be shared verbally in an ad hoc way. It is important that the need to retain confidentiality is not compromised and a breach occurs.

So, following these simple practices will make ensure the confidentiality of the information that you use;

- Consider your **surroundings** when discussing a matter that relates to a person particularly if it is sensitive and think about having a confidential discussion with someone in a location where you won't be overheard or interrupted.

- Don't leave personal information visible on your desk or in your workspace. **Secure** the information in line with the sensitivity of it but at all times avoid the public display of personal information.

- Be careful who can **overhear** your phone conversations

- Always **lock your screen** when you are not present at your computer

- Shred or **securely dispose** of information which is no longer needed

- **Verify** the identity of the person calling or emailing before you give out information

- Password **protect** / encrypt emails containing sensitive data or use programmes specifically designed to be secure.

7. Disposing of Confidential Waste

Organisations have received big fines for failing to dispose correctly of personal data. Examples include filing cabinets being abandoned whilst still containing confidential information, or confidential information being discovered dumped.

Information should be disposed of in accordance with your school's retention policy, the policy will tell you what information should be kept and for how long. Part of the Policy will also discuss the proper procedure for securely disposing personal data.

Given the move to recording on systems rather than on paper, hard copy disposal may be less of an issue in the future. However, historical paper records will need to be disposed of securely.

So, what should go where?

- General non personal information e.g. timetables or newsletters can be disposed of via recycling or general bins but be wary that there isn't sensitive business data such as account or sales details included in them.
- Personal information should never be put in with general recycling or waste. The "value" of the information may not be obvious at first glance, but if it can identify a living person, careless disposal is a data breach. Personal data should only be disposed of in the confidential waste bins or using the approved shredder.
- Confidential waste bags must be logged, securely stored, zip tied when full and only disposed of via approved contractors.
- Extra care should be taken with special category data (eg SEND, safeguarding records, admissions records containing information about a person's religion or ethnicity). Ideally this should be shredded as soon as it is no longer needed.
- Electronic records should be deleted when no longer required,

Where is personal data stored?

- Emails
- Electronic directories
- Filing cabinets
- Apps
- DVDs, CDs, USB sticks and memory cards
- Safes
- Diaries

It is not always straightforward to delete information from electronic systems. If a system is not able to permanently and completely delete all electronic data, it should be 'put beyond use" which means that it is separate and not accessible by normal means, i.e. through SIMS, also no decisions will be made using the information and no other organisation has access to the information.

Your IT team and DPO will be able to help you work out how to put data beyond use.

8. Data Protection Rights

Just like the previous Data Protection Act, GDPR and the Data Protection Act 2018 give individuals rights over their personal information. There are 7 such rights, and all must be complied with or the person making the request must be responded to within 1 month. A request can be verbal or in writing but ideally a verbal request should be followed up in writing so that there is no confusion.

This can be a particularly complex area so if you receive what you think constitutes any of the follow you should raise it with the Data Protection Lead or DPO.

Right to be Informed. This means that when you take personal data from someone or receive it from another source the person must be told the certain things such as what information, how it will be processed and why. All of this is generally covered by the School's Privacy Notice and must be given at the time the information is captured or as near to as can be.

Right of Subject Access. Subject to some limited exceptions individuals have the right to know what information is held about them and have a right to access it. A separate briefing covers this as it is one of the most important rights to be aware of.

Right to Rectification. Individuals have the right to ask to rectify information they think is inaccurate and have the right to ask us to complete information you think is incomplete. Opinions are, by nature, subjective. As long as the record is clear that the data is an opinion and, where appropriate, whose opinion it is, there may be a good argument for not rectifying the entry.

Right to be forgotten, also known as the right to erasure. This right applies in certain circumstances particularly when the basis relied on for processing is consent or if it is no longer needed. If the school is processing the data on the basis of legitimate interests or public task and an objection is received, the school must weigh the individual's objections up against the school's interests in continuing to process the data. You may need to stop using the data whilst you are deciding on whether this right applies.

Where images have been distributed as part of printed materials, the school is not expected to retrieve these provided that there was consent at the time that they were distributed.

Right for the restriction of processing data. Individuals can ask organisations to temporarily limit the use of their personal information when they do not want it deleted, for example they are considering a legal claim and do not want it deleted.

The right is exercisable when the individual is making a challenge to the accuracy of the information or objecting to the use of their data

Right to object to processing. Individuals have the right to object to processing if the information is processed as part of the School's legal tasks a public task or is in the School's legitimate interests.

Right to data portability. This only applies to information provided by the individual (or gathered through apps) who has the right to ask that their electronic personal information is transferred from one organisation to another.

Rights in relation to profiling or automatic decision making. It's not likely that this will apply in the School but may do if an aptitude test is carried out and a decision is made about the person taking the test with no input from a human. In this case the individual has a right to have a human review any decision made automatically.

9. The Right of Access (Subject Access Request/SAR)

The Data Protection Act 2018 and GDPR gives people the right to know that you are processing information about them, and the right to request information that is held about them. This is known as a Subject Access Request (SAR).

You might receive a request for "all information that the school holds about my son, and in particular any correspondence, notes or emails relating to his ……."

Or you might receive a request from the pupil themselves if the student is over 12 or 13 and able to understand what they are asking for the request should come from them directly.

Requests do not have to be in writing nor state that they are a subject access request. They could be verbal, received via email, social media – but it is always best to ask that any verbal request is put in writing or respond to the requestor clarifying their request so that there is no confusion about the date when it is received or what is being asked for. You can put this in an email or use a specific form.

If you receive a SAR time is of the essence pass it immediately to your Data Protection Lead. Requests must be responded to within one month of receipt either with the information that they have requested or that you may need to extend the response time.

This month does not start to run until you are sure that the request is from the person they say they are and so an identity check should be done unless this is not obvious, you may want to have them provide a copy of identity or present it to the reception desk. Your internal data protection lead will help with this.

If there is a need to clarify the scope of the request, this does not stop the clock unless you are unable to understand the request. The one month time limit is subject to a very limited number of exceptions where the collation of records is complex, this does not include the administration time and must be absolutely justifiable as the requestor may challenge it through the Information Commissioner's Office (ICO) No extra time is allowed for school holidays either!

You will then need to search your records (paper and electronic) for relevant information and help to identify who else may hold information. Your internal data protection lead may co-ordinate this.

You should discuss with your data protection lead any concerns you may have about disclosing the information – for example whether it may put someone at risk, whether other agencies are investigating concerns for example social care or the police, or whether it would reveal information about third parties.

If you are a maintained school be aware that there is another right which entitles students and their parents to access the educational record within 15 working days.

10. Consent

Consent is one of the legal bases for processing personal data. It is used when there isn't any law or legal requirement for you to collect personal data, it is for situations where you would like to do something that will use personal data such as conduct a survey where you need to identify people, take pictures of them for business purposes or if they join a club and have to provide personal data. GDPR says that consent must be;

- Freely given - consent means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given, and it will be invalid
- Specific - one of the major changes with GDPR is that organisations can no longer "bundle up" consents – for example one question combining agreement to images being taken for internal use and for external marketing materials. Individuals have the right to pick and choose whether to consent to each use of their data.
- Informed - when seeking an individual's consent to processing data they need to know the following:
    - What their information will be used for, how it will be used and why you need it. You need to make this clear on your form, and ideally link through to your Privacy Notice on your website or signpost it.
    - How long the information will be retained for. This should reflect your retention schedule. You should tell individuals about this when you collect their consent.
    - Whom the information will be shared with (if anyone). Examples of this could be with an organiser of an activity or a photography company. If this is the case, you should check that you have a contract in place with the third party and that they are GDPR compliant.
    - There must be an option to withdraw consent at any time and withdrawal of consent must be as easy as the process of giving consent in the first place. For this reason, you must provide details of how to withdraw consent – for example a school contact email address. When consent is withdrawn, the school should act on this as soon as practicable. This will not affect the lawfulness of processing up to that point. There must be no detriment to the individual as a result of withdrawing their consent.
    - An unambiguous indication of the individual's wishes by which he or she, signifies agreement to the processing of personal data relating to him or her". This could be a tick box but not one that is pre-filled

Consent to processing personal data is often confused with permission to take part in a school activity – for example face painting, a trip, or the use of the internet as part of the school curriculum.

This is a tricky area, but one that you should be broadly aware of. Refer to your data protection lead who can consult with One West, your external Data Protection Officer if there is any doubt.

11. Data Minimisation

One of GDPR's principles is data minimisation, this is another way of saying only process the minimum personal information that you need for the purpose.

In schools this really translates to the safe keeping of student's information, and not sharing more than is needed. Each school must decide on its own procedures, but we would recommend:

In primary schools

- Only put first names on pegs
- Don't display full names with pictures on display boards e.g. celebrating awards
- Don't put up birthday lists on walls with pictures of the child

In all schools

- Under most circumstances don't publish a child's full name with a picture in the media – unless there is a very good reason to do so and you have explicit consent on this.
- Ensure that medical information, in particular, is out of the sight of those who do not need to see it. Schools should adopt a risk- based approach – for example caterers may need to have sight of a picture of the child with their name but should not have this in full view of students
- Consider what medical information you need to take on a trip – more information may be needed on a residential trip than a short outing. It may be that only student initials are used, or other identifier so that their identity is protected if the information is lost. This must be balanced against the need to ensure their medical safety.
- Keep personal information secure – for example SEND information in a SENCO's office should not be left lying on a desk, trip packs should be disposed of securely (shredder or confidential waste – insert your arrangements) and not left lying around
- Only share information about students where there is a need to do so – for example identify who needs to know safeguarding information – it should not be shared beyond this.
- In the case of online diaries, consider who has access to the information and what they should be able to see – anonymise entries where possible if they relate to sensitive information for example social care visits or health appointments
- Consider who has access to folders on the school system and related programmes – for example write permission may be appropriate but not read.
- If you receive requests from agencies for information about students – for example surveys or statistical information – consider whether the information could be anonymised. Consult with One West your Data Protection Officer if you receive such requests.
- Are you collecting more information than you need in a visitor book? i.e. only collect car registration numbers if you have car parking on site. Make sure that your system for recording visitors is out of full view, and people who do not need to know can't see the information – for example names of visitors, reasons for visits. We provide separate guidance on this.
- Do not display passwords where they can be seen by others.

12. Data Protection by Design

The GDPR introduced a new concept of “data protection by design”.

What does this mean?

Whenever you are thinking of introducing a new way of processing personal data, you need to ensure that data protection is a part of this process – rather than an afterthought at the end.

What should you do?

When thinking of any new process that could impact on data protection, **before purchasing or implementing it** think about how to incorporate good data protection principles in particular, the security of data, how individuals can consent or have their data erased in appropriate circumstances and whether the use of the new process is going to be proportionate.

Examples of this are:

- Sending out a new form that asks for personal information – are you telling people if providing their info is mandatory? Are you telling them how they withdraw consent if the information is being gathered in this way? How would you erase the data if requested and if there was a legal basis to do so?
- Introducing cashless catering or other use of fingerprints. Have you advised of a reasonable alternative if people don’t agree? Is the use proportionate and have you told people what the data will be used for – for example entry panel doors could use fingerprints simply for access purposes, but you could not use this information for other purposes e.g. attendance monitoring unless you have consulted on this, assessed whether it is proportionate and informed people.
- CCTV – the siting of new cameras. Where are they placed, and do they intrude unnecessarily on people’s privacy? Have you put up notices and told people?
- Buying a new programme – for example for safeguarding or a new app for students? Have you checked to see how the information is used and shared? Have you told students / their parents about it? Can the information be erased if so requested and if it was provided on the basis of consent?

If you are introducing a high risk process – for example using lots of records (eg more than 1000), using sensitive personal data (eg SEND, safeguarding, health) or the use of CCTV, the school **must first** do a risk assessment (data protection impact assessment). The idea is to identify any issues before you start using the new system. Speak to your data protection lead (insert name) who will contact One West, the schools outsourced data protection officer and who can give advice.