Information Governance Unit: InfoNotes

Data Protection Guidance for Schools and Early Learning and Childcare Settings (ELC)

Schools and ELC settings process personal data every day. From taking the register, collecting lunch orders, organising trips, managing tests and exams, arranging parents' evenings, recording pastoral notes, managing family relationships, displaying school photographs, using CCTV, and being aware of allergies – personal data is part and parcel of school life.

Data protection legislation provides a governance framework through which personal data can be collected and used fairly and lawfully. It enables organisations, like schools and ELC settings, to do what they need to do with personal data whilst ensuring that people's privacy is respected and everyone understands what will happen to their data.

There are six data protection principles which organisations must comply with. If you comply with these, you will not breach data protection legislation. This guidance addresses each principle, and provides practical advice on what they mean and how they might apply to a school environment. It highlights the statutory rights people have in relation to their data and how requests to exercise those rights should be handled. It also provides advice on when to conduct Data Protection Impact Assessments, when you might need an information sharing agreement, and also what to do if something goes wrong and you suspect a data protection breach has occurred.

There is a checklist for Headteachers, Head of Centres and Business Managers at the end (Appendix A); however if you have any questions about the content of this guidance, you should talk to your manager or contact the Information Governance Unit at:

information.compliance@edinburgh.gov.uk.

1. First things first… Definitions

Personal data means:

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Basically, if a person can be identified from the data, or if the data is a unique reference or identifier of one person, then it will likely fall into the definition of personal data. Examples will include (but are not limited to) names, addresses, email addresses, dates of birth, pupil numbers.

Special Category Data is personal data which is considered more sensitive than normal personal data and deserving of extra protection. It includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Processing refers to 'doing something' with personal data which might include collecting, storing, sharing and deleting it.

2. What next?... Understand the Data Protection Principles

The Data Protection Principles set out the basic rules which, if followed, will enable schools and ELC settings to comply with their data protection responsibilities. These require that:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Personal data is adequate, relevant, and limited to what is necessary
- Personal data is accurate and, where necessary, kept up to date
- Personal data must be kept for no longer than is necessary
- Personal data must be processed in a manner that ensures the appropriate security

In effect this means that schools and ELC settings should:

- Know that what they are doing with personal data is lawful;
- Tell people why they need the data they collect, and what they will do with it.
- Only use personal data for the reason they collected it, and not use it for any other purpose without first re-visiting the above points.
- Only collect the personal data they need.
- Have reasonable procedures in place to ensure personal data can be kept up to date if it is likely to change over time.
- Apply the Council's record retention rules, so personal data is disposed of consistently.
- Identify appropriate security measures to protect personal data from unauthorised access or loss. This includes ensuring it is only accessed and used within the EU.

To keep yourself right, you may wish to consider your processing activities through the following prism (see Appendix C for practical examples):

Reason	What is the lawful reason for the processing?
Expectation	Will the data subjects (or their representatives) expect their personal data to be used in this way?

Documentation	Is there sufficient documentation in place to ensure personal data is treated consistently and compliantly?
Security	Are there sufficient security arrangements in place to keep the personal data safe?

3. What does that really mean?

1. Processing personal data lawfully

As highlighted within the introduction, schools and ELC settings will process personal data for a variety of reasons. The reason for doing something with personal data (the purpose) will determine the lawful basis which allows you to do what you want to do.

The lawful basis is also known as a 'condition of processing', and there are various options available under data protection legislation. See InfoNote: Conditions of Processing for more information on all the conditions available.

Appendix C provides a table of practical examples of how these will apply within schools and ELC settings, however the main conditions of processing which are likely to be used, and the reason they will apply, are explained below.

- **The performance of a public task, carried out in the public interest, or as part of the Council's official authority**.

  This condition will apply to the majority of personal data processing which schools need to do to deliver education. This 'public task' is underpinned by the Education (Scotland) Act 1980 which provides a general statutory duty to provide education but does not dictate specifically how that is to be achieved.

  When teachers, practitioners and support staff collect and use personal data as part of delivering 'the day job', their reason for doing so will be to fulfil their duty to deliver education. Consequently they are completing the Council's public task. Examples will include collecting data for the school or centre roll, managing pupil records, mark books/records, entering personal data into apps to advance learning, collecting statistics required by Government, organising parents evenings, facilitating free school meals, P7-S1 transition meetings, or sharing career path discussions with Skills Development Scotland. Although not directly referred to in legislation, all these activities are about delivering an effective education service and/or positive learning environment.

  When using this condition, schools and ELC settings must ensure that they have designed the process in such a way that meets all the data protection principles and respects data subject privacy. If schools/settings are unclear whether a process does comply with data protection legislation, they should assess it using a Data Protection Impact Assessment (DPIA).

If the process is mandated corporately, e.g. use of EE2 forms or collection of data for Scottish Government, then individual schools and ELC settings will not be expected to complete DPIAs. Where necessary, these should have been done centrally. However, if a school is introducing a new process locally, e.g. introducing a new app that is not used elsewhere and so has not been assessed, they will need to conduct their own DPIA to provide assurance that the data processing complies with the data protection principles.

- **It is necessary as part of a legal obligation, or contract**.

  This condition will apply when a piece of legislation, or a contractual term, specifically directs that personal data must be dealt with in a certain way.

  Examples of when a legal obligation will apply is when the school must complete a Child's Plan, when the Council receives a court order, or the Council has to refer certain complaints to the GTCS.

  A contractual obligation might apply if, for example, the school or the Council has signed a contract requiring personal data to be collected or shared in a particular way e.g. where school clubs are conducted onsite, the school may need to know the details of all staff members in order to manage emergencies. Where this is set out in a contract, it is permissible to exchange the data.

  Remember, if you are processing personal data because it is necessary for a legal or contractual obligation you do not need to also ask people's permission. It is important to manage people's expectations: you should tell them how personal data will be processed, and explain why, but you do not additionally require their consent to share it. For example, when organising a school trip it may be necessary to share personal data from EE2 forms with the host/trip organiser to enable them to manage their duty of care. If pupils/parents are not happy to provide personal data which is necessary under the contract, the pupil will not be able to go on the trip.

- **It is necessary to protect somebody's vital interests**

  This condition of processing will apply when you need to share personal data in 'life or death' situations. In practice, this means for the purpose of child or adult protection.

  This condition will apply to both cases where you know for a fact that there is a child/adult protection concern, and where you need to share personal data in order to establish whether there is. It does not, however, automatically cover the sharing of Wellbeing Concerns where these relate to lower level concerns which are not considered to be child protection. If personal data needs to be shared for Wellbeing, this is more likely to fall within the Council's public task, and may also require consent. See GIRFEC Practitioner's Guide for more information.

- **The data subject, or their parent/guardian, has given consent for their personal data being used in that way**.

  Consent should not be used in any cases where there is no practical alternative to processing personal data in a particular way, or where there can be considered to be an unfair balance of power between the data subject and the controller. In these cases, a different condition of processing is likely to apply. However, consent may be required where a school or ELC setting would like to process personal data in a particular way which could be considered to be beneficial, but not essential, and for purposes where people would generally expect to have a greater say in what will happen to their data.

  Examples of when consent will be relevant will include when biometric data is used to pay for school lunches, or when pupil photographs are published beyond the immediate school environment e.g. in newspapers, on school websites or social media.

  Where consent is used as a condition of processing, it needs to be explicit and evidenced, it must also be given by some affirmative action like completing a form, or clicking a button. Consent cannot be assumed through a lack of action, so it is not acceptable to automatically assume that consent exists unless someone tells you otherwise. If you process on consent, you must also be aware that individuals can withdraw their consent at any time and you will need to make it easy for them to do so, you may also need to delete their personal data if they ask you to.

  Do think carefully before deciding to use consent as a condition of processing under data protection because, by its nature, it provides additional rights to data subjects which may not be easily supported within schools and ELC settings. In many cases, the public task condition could equally apply and might be preferable to use. Seek advice from your Manager and/or the Information Governance Unit if required.

  If consent is to be used, children aged 12 and over will normally be considered mature enough to be able to consent to their data being processed in a particular way. Where a child is under 12, consent should be sought from their parent/guardian. The age of consent rises to 13 if the processing relates to an online service delivered directly to children. If schools or ELC settings deliver online services, it is likely that the public task will be more appropriate however do consult the Information Governance Unit if you are unsure.

  NOTE: consent should still be sought in relation to the sharing of Wellbeing Concerns that are not related to child protection. Although, in data protection terms, this processing will be covered by the Council's public task, consent is still required in these circumstances to ensure that we act in accordance with people's human rights. As above, consent must be explicit, and evidenced/recorded. See GIRFEC Practitioner's Guide for more information.

Occasionally, it might also be necessary to process personal data for the prevention and detection of crime. It is OK to give the police, or other law enforcement agencies, personal

data if they ask for it. These requests should normally be directed to the Information Governance Unit unless, in the circumstances, the personal data is urgently required. See InfoNote: Information Sharing (Requests for the Prevention and Detection of Crime) for more information about how to deal with these types of requests.

2. Telling people what you do with their data

It is important that people understand why a school or ELC setting collects personal data and what they will do with it. This manages expectations, and builds trust by ensuring that people are not surprised by what happens to their data. Data protection legislation requires us to tell people what we will do with their personal data through a privacy notice.

A privacy notice could be a leaflet, a web page, or a statement on a form. The Council has published a detailed privacy notice on its website, and a standard privacy notice has been produced which schools and ELC settings can adapt for their own websites and handbook. See Appendix B.

Where a school or ELC setting needs to collect data on a corporate form, e.g. EE2 forms, privacy information will be provided within them. However, if you are collecting personal data for a purpose which requires you to create your own form, you must ensure that you explain why the personal data is required and what you will do with it. You should include a link or reference to the Council's privacy notice where people can learn more about what the Council does with their data. See InfoNote: Privacy Notices.

As schools and ELC settings will be processing childrens' personal data, privacy information should be expressed in language that children will understand. As they are the people who will be impacted if things go wrong, they should have as full an understanding as possible of how their personal data will be treated.

The Council also publishes a Record of Processing which details all the activities that the Council does which involve processing personal data. It is recommended that you provide a link to the Council's Privacy notice and Record of Processing on your school or establishment website.

3. Collecting personal data

When collecting or using (including sharing) personal data, it is important to only use what is necessary for the purpose. Always evaluate what information is relevant, proportionate, and necessary and don't process more than you need.

If some personal data is essential, and other information is helpful but not essential, the difference should be made clear to the data subject so they can decide how much information they are comfortable providing. This can be explained within your privacy notice.

4. Keeping it accurate

Data protection law requires organisations to have reasonable measures in place to ensure that the personal data they use is accurate and up to date, particularly when the information will be held for a period of time over which it might change.

Accuracy can be checked as part of business as usual processes, or as routine distinct exercises. The frequency of routine exercises will be influenced by the likelihood of the data changing and the impact on the data subject if the data held is wrong. Schools normally check the accuracy of the personal data they hold annually at the beginning of each school year. This is appropriate, and meets the requirements of the legislation.

It is important that inaccurate data is updated when it is known to be wrong. Schools and ELC settings should ensure that they are able to update their records timeously should they be informed that the personal data they hold is no longer correct. Inaccurate data will be any personal data which is factually wrong, e.g. incorrect date of birth, change in emergency contact number. There is not an obligation to change records that the school or ELC setting considers to be correct, but which the data subject (or their representative) disagrees. This might happen, for example, if minutes of a Child's Planning Meeting is disputed. Although you do not need to correct the record in these circumstances, it will normally be good practice to record the fact that they are disputed and why. See InfoNote: Accuracy of Personal Information.

5. How long to keep personal data

Personal data should not be kept for longer than is necessary for the purpose for which it was collected. The Council's Record Retention Schedule sets out the time periods which certain records need to be retained for, and after which they should be disposed. These rules have been agreed by Services and are influenced either by legal obligation or business need. They should be applied consistently to both paper and electronic records.

When schools or ELC settings destroy records in accordance with the retention schedule, they should record the destruction within a Disposal Register. For further guidance see: Orb page: Overview of Records Management.

Please note that records of enduring historic value to the Council and the communities it serves will be exempt from this principle and must be transferred after business requirement to the Council's archives service – Edinburgh City Archives. For further advice and information please contact the Archives team at archives@edinburgh.gov.uk / 0131 529 4616.

6. Keeping personal data secure

Schools and ELC settings need to have reasonable measures in place to protect the personal data they store and use. This does not mean that all staff have to do exactly the same thing if that is not practical. Schools and ELC settings can set their own standards in relation to

where personal data is stored and accessed based on the particular demands they have, but all staff should understand the working practices within the school or the setting, and these should be documented wherever possible, to ensure that personal data is treated consistently.

Security can be managed by adhering to Council policy and local procedures. All staff should have completed the Information Governance e-learning module which provides general information about responsibilities. At school or establishment level, practices to protect personal data should be reinforced internally so everyone understands how colleagues are expected to manage and protect personal data. It is recommended to document local processes in place, and talk about where these are, or what is expected, within school or establishment meetings as relevant. This will ensure that everyone has the same understanding, and knows where they can seek advice if necessary. In doing so, it is easier for everyone to recognise that complying with data protection principles is something that they do anyway; it is not an added on extra which they need to fear.

Within the school or the ELC setting, appropriate security measures may include keeping PPR files in locked storage, using G:drive folders with controlled access permissions, having clear rules about what information can and cannot be taken home, and ensuring that any removable media used (e.g. USB sticks) is encrypted or otherwise follows Council policy and procedure. If it is not possible for a school/ELC setting to follow Council policy/procedure in a way which may have an impact on the security of personal data, the establishment should report the matter as an information risk using the Council's Risk Management framework. See Section 7: Information Risk.

Protecting personal data can get more complicated if it needs to be shared outside the school/setting environment. For example, if personal data needs to be emailed to another organisation, it is important to consider whether the transmission is secure and what the impact would be on the individual if the personal data was exposed. Although some email addresses, such as those with .gcsx, .pnn, or NHS.net, are secure, many are not. It is important to consider how personal data can be safely exchanged electronically and seek further guidance from ICT Security if required.

Equally, if a school or ELC setting independently wishes to introduce a new system or app which will use or store personal data, its security must be assessed to ensure that the Council will not breach data protection legislation by using it. In particular, it is important to understand whether the system is vulnerable to malware, and also where the data is going to be stored as data protection legislation requires personal data to normally only be processed within the EU. Failure to ensure that the personal data is appropriately secure will result in the Council breaking data protection law and committing a data protection breach.

Systems/apps which process personal data should be assessed using a Data Protection Impact Assessment (DPIA). This will assess all data protection principles (not just security). Depending on the circumstances, it may be necessary for specific security information to be provided by the supplier, or security assessments to be carried out. The system might need to be Penetration tested, or require a Short Form Assessment. For further information, see InfoNote – Penetration Testing.

In terms of systems and apps in current use, these have been initially assessed to understand their compliance status in relation to the data protection principles. A list of apps which have undergone an initial assessment is included at Appendix D. **This list will be updated and a revised version circulated prior to 25th May 2018.** Where an app/system has been assessed as unlikely to comply with data protection legislation, it should no longer be used in schools and ELC settings unless they can do so without entering any personal data (remember, personal data includes any unique identifiers, e.g. numbers, which are used to identify individuals). If a school chooses to use a system/app which is not listed, they must complete their own DPIA.

If personal data is shared routinely with other organisations, the Council will need to have an information sharing agreement in place. This documents when personal data will be shared, why, and how. When establishments are involved in routine data sharing, they should be assured that a relevant information sharing agreement is in place. If the Council has a corporate relationship with the organisation there should be a central agreement in place (establishments should check); if the sharing is part of a unique local relationship, the establishment will need to create their own information sharing agreement. For further information, see Information Sharing Agreement Procedures.

4. How do I know I am doing this right?

Schools and ELC settings can be sure that personal data is being processed appropriately by conducting a Data Protection Impact Assessment (DPIA). This is a process which helps identify and minimise data protection risks. Completing a DPIA will provide assurance that your processes comply with all of the data protection principles. It will also highlight what governance documentation is required, e.g. Penetration Test, Information Sharing Agreement, Privacy Notice. For further information see: Data Protection Impact Assessment Procedures.

5. What should I do if it all goes wrong?

Don't panic! Sometimes things do go wrong, and personal data ends up somewhere that it should not. This is known as a data protection breach and might include, for example:

- Personal data being lost, stolen, or accessed in a way it should not have been. This might be through the loss of hardware (e.g. laptops, portable devices) or paperwork containing personal data
- Emails sent to multiple people showing their private email addresses
- Disclosure of personal data in error (e.g. a letter or email sent to the wrong person, or personal data given over the phone to someone who should not receive it.)

The important thing is to recognise the problem quickly and report it in accordance with the Council's Data Protection Breach procedures.

The Information Governance Unit will be able to provide specific advice but, generally, we should do what we can to ensure that people are not harmed or disadvantaged as a result of the breach. We should also let people know when something has gone wrong, so they are informed and can take any steps they feel necessary.

It is essential that you report a potential data protection breach as soon as you become aware of it. Certain breaches, where there is a high risk of people being impacted as a result of the breach, require to be reported to the ICO within 72 hours of them becoming known to the organisation. The Information Governance Unit will assess whether a breach needs to be reported to the ICO so it is vital that you involve them as soon as possible so they can help and advise.

Use the Data Protection breach form to report a data protection concern. It is on the front page of the Orb in the 'Report it' box.

For more information, see the Data Protection Breach procedures.

6. Individual Rights

Individuals have certain rights under data protection law, these include the right to ask what information is held about them, to ask for their personal data to be rectified if it is inaccurate, or, in certain circumstances, not to be processed further or deleted. The main rights which might manifest in a school and ELC environment are:

- Right to access personal data
- Right to rectify personal data
- Right to erasure, also known as the right to be forgotten

If you are at all unsure how to deal with a request you have received, you should contact the Information Governance Unit.

Right to access personal information

It is accepted that a school or ELC setting will share personal data with parents as part and parcel of their day job (their public task), and the following is not intended to prevent dealing with business as usual situations. However, establishments will sometimes receive requests which require a statutory response, either under data protection legislation, or the Pupils' Educational Records (Scotland) Regulations 2003 which provides parents and guardians with a right to access their child's educational record.

Examples of the different types of request which might be received, and how to deal with them, are listed below. If you are unsure how to deal with a request you have received, consult your manager or contact the Information Governance Unit.

- **A parent requests a copy of records relating to their child's education e.g. test results, timetable, school report**

  Requests from parents for information which is directly related to their child's education should be handled in accordance with the Pupils' Educational Records (Scotland) Regulations 2003. These requests should be answered directly by the school within 15 school days. See: Parental Access to Pupil Records.

You do not need permission from a pupil to disclose their educational record to their parent under these Regulations, however, if you are aware of strains within the family which may result in the young person suffering harm or distress by the disclosure, you should consult them (or their representative) to understand their view. If you consider that the young person will suffer harm or distress, an exemption to the parent's right of access might apply and you should consult your manager or the Information Governance Unit.

Such requests should not normally involve the personal data of other children, however if personal data of other children (third parties) are included, this should be redacted/blacked out prior to disclosure. If you are unsure about what information should be disclosed, consult your manager or the Information Governance Unit.

- **A pupil or parent asks for all personal data which is held about them by the school. The information held goes beyond information which could be considered their educational record, or data that you would disclose under business as usual. It may include, for example, records about health, family situation, complaints and/or concerns which have been raised.**

  These requests are more likely to fall within a person's 'subject access' right to access their personal data under data protection law. These requests must be forwarded to the Information Governance Unit – Information Rights Team who will answer them directly.

  The IGU may require you to send them a copy of the information requested, and you should advise them if you have any concerns about the information being shared with the data subject in the circumstances.

  These requests can be made verbally, although it is helpful if a person can write down the information that they would like to receive so there is no misunderstanding. Standard requests must be responded to within one month, however the timescale to respond to complex requests can be extended to three months if necessary. The Information Governance Unit can provide more information and advice about subject access requests.

  Note: under subject access, an individual only has a right to receive their own personal data so, if there is information which relates to other children contained in the records requested, it will be redacted.

- **A parent is worried that their child is being bullied, and wants to know how they are in school, and who they are associating with.**

  This kind of enquiry is part and parcel of school life and should be managed, at least initially, as business as usual following school procedures in relation to the concerns raised.

Only if a more formal request for documentation is made might the above rights be engaged. If you are unsure how to manage a situation or whether a subject access request has been made, consult your manager or the Information Governance Unit.

Right to rectify personal data

See principle 4 relating to accuracy, and the need to keep personal data up to date through business as usual activities. If an individual is unhappy about what information is held about them at school, and wishes to complain in relation to their data protection rights, the matter should be referred to the Information Governance Unit – Information Rights Team who will respond to it.

Right to erasure / to be forgotten

This is not an absolute right, and will only apply in limited circumstances. The right to erasure is intended to help protect individuals from their personal data being misused by organisations, and to protect them from the impact over-retention of personal data might have on their privacy. It normally relates only to processes which are based upon consent.

Where personal data is processed within school or ELC settings for a purpose which is based on the Council's public task, a legal obligation, or a condition which is not consent, the right to be forgotten is unlikely to apply. In these cases, a person's right around over retention is protected by, and managed through, the application of the Council's Record Retention Schedule.

Where a process is based upon consent, e.g. publishing pupil photographs, the right to be forgotten may be more likely to apply; it is important to recognise this when deciding whether to use consent as a condition of processing under principle 1.

Where a school receives such a request for erasure, it must be forwarded to the Information Governance Unit – Information Rights Team to respond to.

7. Information Risk

It is recognised that there may be circumstances that arise or exist within school or ELC environments which may mean that data protection principles cannot be applied as strongly as the establishment would wish. This might apply, for example, if there is an insufficient amount of locked storage, or if personal data cannot be managed in accordance with Council policy or procedure.

If this happens, the matter should be reported as an Information Risk using the Council's Risk Management Framework. This will enable the matter to be fully assessed, and the risk to be recorded, managed, and monitored appropriately.

8. Training and Resources

To assist all Council services in understanding data protection, the Information Governance Unit runs the following workshops which can be booked through MyHR:

Data Protection & You – an overview of the data protection principles, what they mean, and the Council controls which should be used to achieve compliance.
Data Protection Impact Assessment Workshop – a session designed to assist authors who are, or will need to, write a Data Protection Impact Assessment (DPIA).

There are two **e-learning modules** available on CeCil. The Information Governance module (under Council Policies) should be completed by all staff. There is also an Information Governance module for Managers (under Essential Learning for Managers) which provides guidance on Council policy and procedures and when they should be used. A new module on the General Data Protection Regulation is also in development and will be launched soon.

There is a lot of guidance material which can be accessed on the Information Governance Orb page including:

Teach Yourself: General Data Protection Regulation booklet

Data Protection Impact Assessment Procedures, form, and guidance
Information Sharing Agreement Procedures, template, and guidance
Data Protection Breach procedures

We have also produced a series of **InfoNotes** which breakdown specific topics into bite size chunks. InfoNotes are published on the Orb and include:

GDPR & the Data Protection Act explained;
Glossary of Data Protection terms;
What is Personal Data?
Conditions of Processing
Privacy Notices
Record of Processing
Accuracy of Personal Information
Penetration Testing
International Transfers
Individual Rights

Guidance on the Council's Records Management policy and procedures are also available on their Orb pages.

Finally the Information Governance Unit can always be contacted for support and advice. We can also provide bespoke training sessions or briefings if requested. We can be contacted via the following routes:

General data protection enquiries, including questions about procedures and requests for training should be directed to the Information Compliance Team at: Information.Compliance@edinburgh.gov.uk.

Enquiries about Information Rights, including subject access requests, freedom of information requests, or requests to rectify or erase personal data should be directed to the Information Rights Team at: foi@edinburgh.gov.uk.

Enquiries about records management should be directed to the Records Management Team at: recordsmanagement@edinburgh.gov.uk

Enquiries about records of historical value, and the City Archives, should be directed to: archives@edinburgh.gov.uk.

Appendix A – Checklist for Compliance with Data Protection legislation (for Headteachers, Head of Centre and/or Business Managers)

To have confidence that your school or ELC setting complies with data protection legislation, follow this checklist. Please Note: Action 1 (re: School / ELC setting Privacy Notice) must be actioned by 25th May 2018.

Ref	Action	Tick
1.	Ensure standard privacy information (Appendix B) is published on your website and included within the establishment handbooks as applicable.	
2.	Consider the level of understanding colleagues have of data protection. Promote the guidance and procedures available, and when to use them, in staff meetings. (Feel free to invite the Information Governance Unit to attend your meeting if you would like an input on the data protection principles and how they apply in schools and ELC settings.)	
3.	Ensure all staff know what to do if there is a data protection breach.	
4.	Ensure relevant staff know what to do if someone wants to access their personal data, or otherwise exercise their data protection rights.	
5.	Consider current processing through the REDS prism (Appendix C)	
6.	Check the systems/apps used in school or ELC settings and ensure they have been subject to a Data Protection Impact Assessment (check Appendix D for assessments being completed by the Digital Learning Team).	
7.	Consider your practices for sharing personal data, either routinely or as one off requests, and ensure that the process is adequately documented so that personal data is treated consistently by all staff and within the reasonable expectation of the people to whom it relates.	
8.	Assess the practices used for managing, storing, and disclosing personal data within school/setting to identify and record any information risks where Council policy and procedure is not being followed. Report these in accordance with the Council's Risk Management Framework.	
9.	Know the IGU is there to help, contact them if you have any questions. They are nice.	

Appendix B – School/ELC Settings Privacy Notice Template

To provide transparency about why schools and ELC settings collect and process personal data, they should publish privacy information to manage both pupil and parent expectations. It is suggested that this information is published on your establishment's website, and in school/ELC setting handbooks if you have them. You may also wish to consider whether you would like to produce leaflets or posters to help convey the information effectively. It is ultimately for the service and/or individual schools to decide how this information is best delivered within their own environment.

Information about how we manage pupil data in schools/ELC settings

[Insert School/Establishment Name] has a legal responsibility to deliver an effective educational programme to its pupils. In order to do this, we need to collect personal data about our pupils/children and their families so that we can help them learn, and keep them safe. The type of personal data we will collect include:

- **Data about our pupils/children and their families**
  This will include the name, address and contact details of the pupil/child and relevant family members. It will also include information about relevant medical conditions, any additional supports which are needed, and their family situation. We need this information to ensure we know our pupils/children and their families, and to ensure we are able to educate them appropriately, and keep them safe.

  We will also collect personal data relating to personal characteristics, such as ethnic group to enable statistics to be reported. We need this information so the Council can ensure it is delivering education appropriately to all its citizens.

- **Data about pupils/children at school/within ELC setting**
  This will include data about progress, assessments, and exam results. It will also include records of attendance, absence, and any exclusions. We need this information to understand how our pupils/children are progressing, and to assess how we can help them to achieve their best.

- **Data about when and where they go after they leave us**
  This will include information about their next setting/school, career paths or intended destinations. We need this information to ensure we support our pupils/children in all their transitions and do all that we can to help their future be a success.

There will be times where we also receive information about them from other organisations, such as a pupils' previous school, the previous local authority where that school or ELC setting was based, NHS Lothian, Police Scotland, Social work, Additional Support Services, and sometimes other organisations or groups connected to a pupil's education. We use this data similarly to the above: to support our pupils' learning, monitor and report on their progress, provide appropriate pastoral care; and assess the quality of our services

When we collect and use personal data within school/ELC setting, and for the reasons detailed above, we will normally be acting in accordance with our public task. Occasionally we are also required to process personal data because the law requires us to do so, or because it is necessary to protect someone's life.

We will also take photographs in school/ELC setting and display them on our walls, and in newsletters and other communications. We do this in order to celebrate and share what we have done, including individual achievements and successes. We consider this use of images to be part of our public task as it helps us build an effective community which supports learning. We will not, however, publish these photographs on social media or in newspapers without permission. Consent for this use will be sought when a pupil/child joins [Insert School/ELC setting Name] and will be kept on record while they are with us. Consent can be withdrawn at any time, please just let us know.

Sometimes we need to share pupil information with other organisations. We are required, by law, to pass certain information about our pupils to the Scottish Government and the Council. This data is for statistical purposes, and will normally be anonymised. It is normally required to enable the Council, and the Government, to understand how education is being delivered and to help them plan for future provision.

If a pupil/child moves schools/ELC settings, we have a legal obligation to pass on information to their new school/education authority about their education at [Insert School/ELC setting Name].

When we record and use personal data, we will only collect and use what we need. We will keep it securely, and it will only be accessed by those that need to. We will not keep personal data for longer than is necessary and follow the Council's Record Retention Schedule and archival procedures when records are identified to be of historical value and require to be retained in the Edinburgh City Archives.

For more information on how the Council uses personal data, and to know more about your information rights including who to contact if you have a concern, see the City Of Edinburgh's Privacy Notice.

Sharing personal data to support Wellbeing

In addition to the above, [Insert School/ELC setting Name] has a legal duty to promote, support and safeguard the wellbeing of children in our care.

Wellbeing concerns can cover a range of issues depending on the needs of the child.

Staff are trained to identify when children and families can be supported and records are kept when it is thought that a child could benefit from help available in the school/ELC setting, community or another professional. You can expect that we will tell you if we are concerned about your child's wellbeing, and talk to you about what supports might help in the circumstances. Supports are optional and you will not be required to take them up.

If it would be helpful to share information with someone else, we will discuss this with you and seek your consent before we share it so that you know what is happening and why. The only time we will not seek consent to share information with another organisation is if we believe that a child may be at risk of harm. In these situations, we have a duty to protect children, which means we do not need consent. On these occasions, we will normally tell you that information is being shared, with whom, and why – unless we believe that doing so may put the child at risk of harm.

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so.

Appendix C – Applying data protection principles in practice (example scenarios)

Knowing whether or not a process complies with data protection principles can be daunting. Here are some example scenarios to help understand how data protection applies to some common activities within schools/ELC settings. Each scenario is assessed under four key areas which we have abbreviated into a shorthand: REDS, to try and help you remember and apply these considerations to other scenarios you deal with.

Reason	What is the reason for the processing? From this, decide what your condition of processing is.
Expectation	Will the data subjects (or their representatives) expect their personal data to be used in this way? Have they been told it will happen through the school privacy notice, or an alternative method?
Documentation	Is there sufficient documentation in place to ensure personal data is treated consistently and compliantly? Documentation might include a local procedure, a DPIA, an Information Sharing Agreement, or a Disposal Register.
Security	Are there sufficient security arrangements in place to keep the personal data safe?

Example Scenarios

Scenario	Things to think about…
Collecting, and checking, personal data at the beginning of the academic year.	**R**eason – the processing is necessary for the school/setting to conduct its public function and deliver effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's/ELC setting's privacy notice indicates that certain personal data is required about pupils in the establishment and explains why. **D**ocumentation – the information is recorded on SEEMiS and managed in accordance with Council policy and procedure. **S**ecurity – Personal data is collected on forms sent home in school bags to ensure they get to the right people. The data collected is recorded on SEEMiS as mandated by Council policy. (Seeking assurance on SEEMiS technical security will sit with the education authority)
Keeping a record of marks and/or assessments	**R**eason – the processing is necessary for the school/setting to conduct its public function and deliver effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a

	public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's/ELC setting's privacy notice indicates that certain personal data is required about pupils in the school/setting and explains why. **D**ocumentation – the information might be recorded electronically or manually. All staff should understand what the acceptable methods of recording this information are within their establishment. **S**ecurity – when agreeing practices which are acceptable within school/ELC setting, staff should also have an understanding of how they are expected to keep the information secure.
Collecting, and sharing information for school/ELC setting trips.	**R**eason – the processing is necessary for the school/setting to conduct its public function and deliver effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. Some processing may also be necessary as part of a contractual obligation if the personal data of those going on the trip requires to be shared with the trip host/organiser to enable them to fulfill their duty of care. **E**xpectation – the EE2 form explains what personal data is necessary for the trip and why. This can be backed up, if necessary, by additional privacy information given about the trip within school which can further explain how the other organisation will manage personal data collected/shared. **D**ocumentation – the EE2 is collected and managed in accordance with Council procedure. Where personal data is required to be shared as part of a contractual obligation, the contract should stipulate what personal data is required and the duties imposed on the receiving party to protect it. The Council's standard contract conditions have been updated to reflect this, and further advice should be sought from Procurement or Legal Services if required. **S**ecurity – consideration should be given to how forms are stored and accessed to ensure access is limited only to relevant staff. Depending on the circumstances, the school will define who may need to access the forms. As above, if personal data is shared with a host/organiser, contract terms should stipulate how it is to be protected.
Conducting pupil planning meetings.	**R**eason – the processing is necessary for the school/setting to conduct its public function and deliver effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The

(These types of meetings can vary depending on the purposes. They might include internal meetings, or meetings which include external organisations)	processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's/ELC setting's privacy notice indicates that certain personal data is required about pupils in the school/setting and explains why. Where particular pupils are to be discussed in a way which is not part and parcel of school/setting business, perhaps because additional supports are required, they and/or their parents should have an awareness of this through normal and existing processes for parent/teacher engagement. **D**ocumentation – meetings can be minuted and/or records relating to individual pupils kept in the relevant pupil record. Meetings which involve external organisations should be underpinned by an information sharing agreement. It may also be helpful to consider having a terms of reference so everyone at the meeting understands its purpose, and how personal data exchanged should be treated. **S**ecurity – People at the meeting understand their responsibilities in relation to the personal data which is shared. If personal data is emailed to external organisations, appropriate security is in place to keep it secure.
Providing personal data to another organisation so they can deliver a STEM course.	**R**eason – the processing is necessary for the school/setting to conduct its public function and deliver effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's/ELC setting's privacy notice indicates that certain personal data is required about pupils in the school/setting and explains why. When notifying pupils/parents of the STEM course, additional privacy information should be provided about how the other organisation will manage personal data collected/shared. **D**ocumentation – the data exchange should be underpinned by an Information Sharing Agreement. (If STEM courses are delivered to multiple schools/ELC settings, this might exist centrally). To ensure that personal data is handled consistently, it is good practice for this also to be supported by local procedures. **S**ecurity – the Information Sharing Agreement will indicate the security arrangements to be in place to protect the personal data collected and shared as part of the process.
Managing parents evenings	**R**eason – the processing is necessary for the school/ELC setting to conduct its public function and deliver effective education. This public function is underpinned by the

	Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's/ELC setting's privacy notice indicates that certain personal data is required about pupils in the setting and explains why. Parents and pupils will have an expectation about what happens at parents evenings from their own experience however specific school practices could be explained in the handbook given to parents if necessary. **D**ocumentation – the school/ELC setting will have standard practices to govern how personal data is used for organising a parents evening. These should be documented and understood by all relevant staff. **S**ecurity – Consideration should be given to appropriate security arrangements in place to protect the personal data from unauthorised access. If schools/settings use an app to manage parent evening slots. Such systems will need to have been assessed through a Data Protection Impact Assessment.
A parent asks for details of a yoga class they are running out of hours at the school/ELC setting to be circulated using GroupCall.	**R**eason – GroupCall is designed to enable the school/ELC setting to contact parents in relation to school/setting business and activities which fall within their public task. This reason is not within the school's/setting's public task and no other condition of processing applies so the processing should not proceed **E**xpectation – the use of GroupCall for this purpose would not be within the normal expectations of use so the processing should not proceed. **D**ocumentation – not relevant. **S**ecurity – not relevant.
A parent asks for a list of pupils in their child's class so they can invite them to a party.	**R**eason – The school register is designed to enable the school/ELC setting to know who is in class which falls within their public task. This reason is not within the school's public task and no other condition of processing applies so the processing should not proceed **E**xpectation – this purpose would not be within the normal expectations of use so the processing should not proceed. **D**ocumentation – not relevant. **S**ecurity – not relevant.
A parent / pupil asks for information held about them.	**R**eason – The purpose is to exercise their statutory right. **E**xpectation – As a statutory right, there is an expectation that the school/authority will respond to such requests. **D**ocumentation – Council policy and procedure indicate how requests should be managed and documented. **S**ecurity – The Information Rights Team will manage subject access requests, and can provide advice on disclosing

	information in relation to Pupil Regulations if there is a concern about how this can be done securely.
Publishing photographs of pupils on Twitter	**R**eason – Promoting achievements and activities helps to provide a positive school/ELC environment and effective education. The purpose fits broadly within the scope of a school's/ELC setting's public task but it could not be argued as absolutely necessary for all pupil images to be published in this way if people did not wish to. Schools/ELC settings should therefore base this processing on consent and ask permission for photographs to be published on social media. **E**xpectation – The school/setting's privacy notice indicates that photographs will only be published on social media with consent. The school/ELC setting sends a letter home indicating that the school/setting has a Twitter page and pupil images may sometimes be published. The letter should seek consent for the processing by asking pupils/parents to notify the school of their view. These letters will manage expectations. **D**ocumentation – Where consent is collected, these must be retained so they can be evidenced. Consent must be explicit, and generated by a positive action i.e. returning the form. It cannot be inferred from inaction. It is recommended that the procedure for seeking and recording consent is documented within school so all staff have the same understanding. Schools/ELC setting must also ensure that they can update consents effectively if they are notified that someone has changed their mind. **S**ecurity – Consideration should be given to appropriate security arrangements in place to protect personal data from unauthorised access.
Sharing career paths with Skills Development Scotland (SDS).	**R**eason – the processing is necessary for the school and SDS to conduct its public function and deliver effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's privacy notice indicates that certain personal data is required about pupils in the school and explains why. **D**ocumentation – the data exchange should be underpinned by an Information Sharing Agreement. To ensure that personal data is handled consistently, it is good practice for this also to be supported by local procedures. **S**ecurity – the Information Sharing Agreement will indicate the security arrangements to be in place to protect the personal data collected and shared as part of the process.

The School is contacted by a former pupil who wishes to know the names of their former classmates to arrange a school reunion.	**R**eason – The school register is designed to enable the school to know who is in class which falls within their public task. This reason is not within the school's public task and no other condition of processing applies so the processing should not proceed **E**xpectation – this purpose would not be within the normal expectations of use so the processing should not proceed. **D**ocumentation – not relevant. **S**ecurity – not relevant
A pupil (aged 17) asks for all their photos to be removed from copies of the school newsletter on the school website and in the printed school archive (going back 2 years).	**R**eason – the photographs were taken and published as part of the school conducting its public task/function and delivering effective education. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing was therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. A person's 'right to be forgotten' will not automatically apply to personal data which has been processed for the public task as people's rights should be adequately protected through retention schedules. That said, whilst the inclusion of photographs within a newsletter will fit within public task, their publication on the internet will normally pivot on consent so schools should consider whether their website is the best forum to disseminate the school newsletter. If newsletters are published on the school website, it is advisable to check whether you have received consent for doing so for the images of the children it contains. If a school holds an archive, and wishes to retain photographs for their historical value, a different condition of processing may apply which will enable long-term retention, however, they should consult with the Edinburgh City Archives (see principle 5) for advice on what records should be archived for their historical value beyond the business need of the school. **E**xpectation – the School's privacy notice indicates that certain personal data is required about pupils in the school and explains why. This refers to photographs which are circulated within the school environment. **D**ocumentation – the school should apply agreed retention rules to ensure that personal data is managed consistently, and people's expectations can be clearly managed as per above. Newsletters should be retained in accordance with the Council's retention schedule which states end of calendar year plus 3 year (see Rule: 20.002.005). **S**ecurity – Schools should consider whether it is necessary to publish the school's newsletter on its website, particularly

	if it is also being circulated to families by other means. This is because once personal data is published on the internet it is harder to completely delete it, and therefore apply the retention period noted above. Personal data published on the internet will also have a potentially greater impact than circulation to the immediate school environment.
The end of term Headteacher's/Head of Centre's Message – circulated to all parents/carers by email – contains the names (first and surname) of pupils who have achieved in particular aspects of school life during the term (e.g. sport, academic, volunteering, civic duty).	**R**eason – the processing is necessary for the school to conduct its public function and deliver effective education. Celebrating achievements is part of building a positive and effective learning environment. This public function is underpinned by the Education (Scotland) Act 1980 and other associated legislation. The processing is therefore necessary for the performance of a public task, carried out in the public interest and in the official authority of the data controller. **E**xpectation – the School's privacy notice indicates that certain personal data is required about pupils in the school and explains why. **D**ocumentation – the school will have a list of relevant email addresses for parents/carers which is kept up to date through normal business processes. Procedures for managing these lists, to ensure that the data is used consistently and compliantly, should be documented. **S**ecurity – when emailing, schools should use the Bcc field to ensure that parents/carers email addresses cannot be viewed by all recipients.

Appendix D – List of Apps being DPIA assessed by Digital Learning Team

The following apps/systems have been initially assessed regarding their compliance with data protection legislation.

Apps/systems listed in the first column are considered likely to comply with data protection principles and are approved for continued use within schools/ELC settings, at this time. Where a DPIA has not already been completed, one will be conducted in relation to these in due course.

Apps/systems listed in the second column have been assessed as unlikely to comply with data protection legislation (mostly as a result of data being stored outside the EU). Schools/ELC settings should not use these systems/apps unless they can do so without entering any personal data (remember, personal data includes any unique identifiers, e.g. numbers, which are used to identify individuals).

This list will be updated, and a revised version circulated prior to 25th May 2018.

Systems/Apps assessed likely to comply with data protection principles	**Systems/Apps assessed unlikely to comply with data protection principles.** These can only be used if personal data is not entered.
ABC Music	Active Heinemann Maths
Adobe Spark	Class Dojo
BBC Bitesize	Dropbox
BBC Education	Edmodo
BBC iPlayer	eJass
Big Maths	On the Button
Class Charts	Padlet
Education City	Seesaw
Facebook (follow Council procedure for social media use)	Showbie
GL Assessment	
GTCS	
iDoceo	
Learning Journals	
Mathletics	
Microlib	
My World At Work	
Office 365	
Pebble	
SQA	
SQA My Study Plan	
SQA Solar	
TES	
Twitter (follow Council procedure for social media use)	
University of Edinburgh MyEd	
Wordpress	
www.classtools.net	
YouTube	