UK GDPR – Guidance on Records Management (provided by Business Management Services at HfL)

Adopted by Howe Dell School in Spring 2020

Reviewed: Summer 2024

Next Review: Summer 2026

CONTENTS

Introduction

Please note that this document has been adapted from guidance in the toolkit for schools created by the Information Records Management Society (IRMS), aimed at maintained schools. The aim of this guidance is to provide some consistency of practice in the way in which pupil records are managed across all schools. It includes suggestions on the content of the pupil record, advice on transferring to the next school, and retention and disposal arrangements for both paper and electronic records.

Guidance on Pupil Records

All schools, with the exception of independent schools, are under a duty to maintain a pupil record for each pupil. Early Years settings will have their own record keeping requirements.

The 'Pupil Record', comprised of educational and curriculum records, should be seen as the core record charting the individual pupil's progress through the education system, and should accompany them throughout their school career. This record will serve as the formal record of their academic achievements, other skills and abilities, and progress in school.

Recording and disclosure of information

Pupil records may be held in paper form, or else electronically e.g. as part of the school management information system (MIS). Schools will have their own systems for maintaining pupil records, which may be a combination of electronic and hard copy files.

All information must be easy to find, accurately and objectively recorded and expressed in a professional manner, as pupils and parents have a right of access to their educational record via two possible routes:

1. A request for an educational record. The Education (Pupil Information) (England) Regulations 2005, states that the pupil record must be provided to parents within 15 school days of a request where the pupil is enrolled in a maintained school. This provision does not apply to Academies, independent schools etc.

2. Requests for information by pupils, or their parents are to be treated as subject access requests (SARS) under Data Protection legislation.

Paper Files

The following information is useful on the front of a paper file, if one is held:

- Surname and forename
- Address
- Stored in alphabetical order in the child's class.

The following information is held on the Registration Form inside each individual pupil file so that it is easily accessible to authorised staff. These are held in the filing cabinets and are locked. Record Sheets for all children are held alphabetically in the office files for ease of use during the school day. The following may be held:

- Emergency contact details
- Preferred name
- Names and contact details of adults who have parental responsibility/care for the pupil
- Reference to further information held on allergies/ medical conditions
- Other agency involvement e.g. SEN, speech and language therapist, etc.
- Reference to any other linked files

Contents of the Pupil Record

The table below lists common and potential record types that may form part of the Pupil Record.

Record Type	**Notes**
Record of transfer from Early Years setting	If applicable
Admission Form	
Data Collection/Checking Form – current	This should be checked regularly by parents to ensure details are accurate
Annual written report to parents	
National Curriculum and Religious Education locally agreed syllabus record sheets	
Any information relating to a major incident involving the child	
Statements/Plans, reports, etc. for educational support, e.g. SEN, Speech and Language	Store in a separate area of the record or keep in a separate linked file
Medical information relevant to the child's on-going education/behaviour	Store in a separate area of the record or keep in a separate linked file. CPOMS is used.
Child protection reports/disclosures and supporting documentation	Store in a separate area of the record or keep in a separate linked file so as to limit access to specific staff CPOMS is used.
Any information relating to exclusions (fixed or permanent)	
Specific correspondence with parents or outside agencies relating to major issues	This may be in email form. Once matter is closed save any correspondence that records sequence of events, pertinent issues and outcomes to pupil record. CPOMS is used.
Summary details of complaints made by the parents or the pupil relevant to the child's ongoing education/ behaviour	This may be in email form, see note above. Most complaints records are retained by the school and not as part of the pupil record. May be stored on CPOMS.
Examination Results – pupil copy	Send uncollected certificates back to exam board after all reasonable efforts to contact the pupil have been exhausted
SATS Results	A note of the result should be recorded

Records not forming part of the Pupil Record

The following record types should be stored separately to the main pupil record, as they are usually subject to shorter retention periods (please see the Records Retention Schedule); they should not be forwarded to the pupil's next school:

- Attendance Registers and Information
- Absence (authorised) notes and correspondence
- Parental consent forms for trips/outings
- Accident forms (a copy can be placed on the pupil record if it is a major incident)

- Medicine consent and administering records (this is the school's record)
- Copies of birth certificates, passports, etc.
- Generic correspondence with parents about minor issues (i.e. 'Dear Parent')
- Pupil work, drawings, etc.
- Previous data collection forms, now superseded (there is no need to retain these)
- Photography/image consents (this is the school's record).

Information stored electronically

Those principles relevant to paper records will apply to those pupil records stored electronically. The MIS may incorporate features to enable elements of the electronic pupil record to be deleted in accordance with retention schedules, whilst the remainder of the record remains intact.

Storage and Security

All pupil records and associated information should be stored securely to maintain confidentiality whilst keeping information accessible to those authorised to see it. Electronic records should have appropriate security and access controls in place; equally paper records should be kept in lockable storage areas with restricted access. Not everyone in a school has a need to access all of the information held about a pupil; this is particularly relevant to child protection information.

Transferring Pupil Records

It is vital to ensure swift transfers of information to the new school to ensure appropriate decisions can be made regarding a pupil, using relevant and accurate information.

Weeding

The Pupil Record should not be weeded before transfer, unless any duplicates or records with a short retention period have been included, in which case these can be removed and securely destroyed.

Transfer Process

Howe Dell will contact the pupil's new school to confirm their attendance at the new school before sending any information on. This includes Year 6 children who move to secondary school, and is to ensure the information goes to the correct school.

The following should be transferred to the next school within 15 school days of receipt of confirmation that a pupil is registered at another school:

- Common Transfer File (CTF) from the MIS via the S2S system.
- Any elements of the Pupil Record, held in any format, not transferred as part of the CTF.
- SEN or other support service information, including behaviour, as only limited information will be included in the CTF.

Child Protection information; this must be sent as soon as possible by the Designated Safeguarding Lead (DSL) or a member of their team to their equivalent at the new school. This should be sent within 5 days of confirmation they have started at their new school. This should be accompanied with a 'transfer of safeguarding records form', one part should be returned to Howe Dell as confirmation documents have been received by the new school. Where possible, the safeguarding records will be hand delivered. However, if this is not possible (ie) if the child moves to a school out of the local area, then the information will be

sent for the attention of the DSP and sent by Recorded Delivery. Two DSP's will check any safeguarding information which is sent, ensuring accuracy and removing the risk of a data breach.

Schools must ensure the information is kept secure and traceable during transfer:

- Records can be delivered or collected in person, with signed confirmation for tracking purposes.
- Pupil Records should not be sent by post where possible. If the use of post is absolutely necessary, they should be sent by 'Recorded Delivery' or via a reputable and secure courier to a pre-informed named contact, along with a list of the enclosed files. The new school should sign a copy of the list to confirm receipt of the files and securely return to the previous school.
- If held electronically, records may be sent to a named contact via secure encrypted email, or other secure transfer method.
- If the pupil is transferring to an independent school or a post-16 establishment, the existing school should transfer copies of relevant information only and retain the original full record as the last known school.
- If a request is received to transfer the Pupil Record or other information about a pupil to a school outside of the UK or European Union (EEA), schools should contact the Local Authority or their Data Protection Officer for further advice.

Retention and Disposal

Retention - Transferring school

Responsibility for maintaining the Pupil Record passes to the next school. Schools may wish to retain the information about the pupil for a short period to allow for any queries or reports to be completed, or where linked records in the MIS have not yet reached the end of their retention period and deleting would cause problems.

Certain elements of the record may need to be retained for longer, for example if litigation is pending, or for transfer to the Local Record Office, in accordance with the Retention Schedule. This may include complaints against the school.

Please note: whilst the Independent Inquiry into Child Sexual Abuse (IICSA) is ongoing, it is an offence to destroy any records relating to the Inquiry. It is likely that, at the conclusion of the inquiry, an indication will be given regarding appropriate retention periods for child protection records. More information can be found on the IICSA website.

Retention – Last known school

The last known or final school is responsible for retaining the Pupil Record. The school is the final or last known school if:

- A secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- It is a school at any point and the pupil left for elective home education, they are missing from education or have left the UK.
- The Pupil Record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed. SEN and other support service records can be retained for a longer period of 31 years to enable defence in a "failure to provide a sufficient education" case.
- If a school wishes to retain data for analysis or statistical purposes, it should be done in an anonymised fashion.

Disposal

Pupil records will contain personal and confidential information and so must be destroyed securely. Electronic copies must be securely deleted and hard copies disposed of as confidential waste.

Digital Continuity

The long-term preservation of digital records is more complex than the retention of physical records. In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement.

Where possible, these records should be “archived” to dedicated server space which is being backed up regularly. Where this is not possible the records could be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file, or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.

Flash drives must not be used to store these records as they are prone to corruption and can be easily lost or stolen.

Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed, used as appropriate. Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

Storage of Physical Records

Appropriate Storage for Physical Records

Records must be stored in the workplace in a way that does not cause a health and safety hazard. The area in which records are stored should be secured against intruders and have controlled access to the working space. Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but, for important core records, fireproof cabinets may need to be considered. However, these are expensive and very heavy, so they should only be used in special circumstances. Core records should be identified so that they may receive priority salvage or protection in the event of an incident affecting the storage area.

Safe Disposal

All records that contain personal data, and in particular special category data, must be disposed of in a safe and secure way at the end of their retention period.

Please be aware that under the terms of The Independent Inquiry into Child Sexual Abuse (IICSA) it is an offence to destroy any records that might be of relevance to the Inquiry. This overrides all business, statutory, regulatory or legal retention requirements, including data protection requirements and the data subject's right to erasure. It is anticipated that upon conclusion of the Inquiry, further guidance regarding retention will be published.

Managing Records Retention

All records, in all formats, should be subject to an applicable retention period, as defined by business, statutory, regulatory, legal or historical requirements. All retention and disposal decisions should be documented in a Retention Schedule.

Each school should have a designated staff member with responsibility for ensuring records are retained, reviewed and destroyed in accordance with requirements, and as soon as possible once their lifespan has expired. They will need to determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained for ongoing business or legal purposes.

All records in all formats must be assigned a retention period and disposal date, either upon creation or when they cease to be in active use, in accordance with the Retention Schedule or policy. A system should be implemented to routinely identify records as soon as they reach their disposal date. This may form part of an electronic record-keeping system or a manual system.

Destruction must include all backup and duplicate copies, in all formats. This is especially vital for personal information which may be kept in various hybrid record keeping systems.

Principles of Disposal

Schools must agree a standard procedure for the safe disposal of records. This must be communicated to all employees and regularly reinforced to avoid any possible data breach. Furthermore, if retention periods are not complied with, material will still have to be provided if a Data Subject Access request or Freedom of Information request is received.

The disposal method must be applicable to the content and format of the information. Destruction must be undertaken in a way that preserves the confidentiality of the information and which makes it permanently unreadable or unable to be reconstructed or re-instated.

Special care should be taken when destroying personal, sensitive or commercial information and confidentiality should be paramount at all stages of the process.

Destruction of Records by Type

Paper Records

All hard copies of official records and those containing personal data must be destroyed using confidential methods, rather than being placed in general waste bins or skips, which could result in a data breach.

Specialist companies can provide confidential waste bins and other services to ensure records are disposed of in an appropriate way. The school will retain the responsibility of data controller, as well as the liability for non-compliance caused by the contractor under UK GDPR. However, if the contractor breaches the terms of the contract or acts outside of the school's instructions, it will become liable under UK GDPR. It is therefore essential that schools check the terms of the contract and set out instructions in a Data Processing Agreement on how the school's data must be handled. It is recommended that schools check their insurance to ensure that they are not at undue risk and are adequately covered. For example, if a contractor disposed of confidential waste inappropriately, security was breached, or data was otherwise lost whilst in the care of the contractor.

Third party contractors should be certified to the following:

BSEN15713 – secure destruction of confidential material
BS7858 – staff security vetting
ISO 9001 – service quality
ISO 14001 – environmental management standard
ISO 27001 – information security

Additionally, membership of the following organisations and associations are recommended:

BSIA – British Security Industry Association
FACT - Federation Against Copyright Theft
FTA – Freight Transport Association
FORS - Fleet Operator Recognition Scheme
NAID – National Association for Information Destruction
SafeContractor – health and safety assessment scheme
UKSSA – UK Security Shredding Association

Approved contractors should always provide a Certificate of Destruction, which should be retained with details of individual records destroyed. A secure area must be designated where records can be stored prior to shredding.

Electronic and Other Media Records

Deletion of electronic records should be a managed and auditable process in the same manner as paper records. Records should be routinely identified for deletion and should be authorised by the relevant senior officer. Before deletion, it must be determined that all legal and business requirements have expired, and that there is no related litigation or investigation. Records must be securely deleted in accordance with the school's security policy. Processes must be in place to ensure that all backups and copies are included in the deletion process.

However, 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'. This means it should:

- Not be used for any decision making, or in a manner which affects an individual in any way
- Not be given to any other organisation
- Have appropriate technical and organisational security and access controls
- Be permanently deleted when this becomes technically possible

If information is 'put beyond use' the individual's Data Subject Access right is exempt. However, if such information is still held it may still need to be provided in response to a court order.

The method of deletion should be suitable to the type of information. The school's ICT department or IT provider should be able to advise on the most appropriate method.

The ICO and National Cyber Security Centre (NCSC) make certain recommendations for organisations with regards to deleting, remarking or recycling IT equipment. In accordance with this it is recommended to use an IT asset disposal company that is fully certified with the industry body, the Asset Disposal Information Security Alliance (ADISA).

Transfer of Information to Other Media

Where lengthy retention periods have been allocated to records, the school may wish to consider converting paper records to an alternative format, such as microfilm or digital media, e.g. scanning. The lifespan of the media, and the ability to migrate data where necessary, should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standardised fashion and to ensure the quality of the electronic version. Organisations must be able to evidence that the electronic version is a genuine copy of the original, and that the integrity of the data has not been compromised.

It is recommended that original versions of records be retained for up to six months after transfer to an alternative media, so as to provide adequate time in which any issues arising out of the data transfer process may be identified.

Transfer of Records to the Local Record Office

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Local Record Office. This may be done during the records' active use, or once administrative use has concluded (depending on their condition) access requirements and advice from the Local Record Office. Once records have been transferred, they will continue to be managed in accordance with the Data Protection Act 2018 and the Freedom of Information Act 2000 and will be subject to any applicable closure periods.

The school should retain details of what has been transferred to the Local Record Office to enable their identification, if required for future use.

If a school chooses to keep their archive records on site for use with pupils and parents, they should contact the Local Record Office for specialist advice on storage and preservation requirements.

Note for Hertfordshire Schools

Hertfordshire Archives and Local Studies (HALS) is the local record office for Hertfordshire. HALS is accredited by the National Archives as a Place of Deposit for Public, tithe and manorial records. They are also appointed by the Diocese of St Albans as their Place of

Deposit, and also hold records of other estates and organisations. In addition, they are the place of deposit for archive records generated by HCC (and its predecessors) as well as the district councils (and their predecessors).

For more information, email hals.enquiries@hertfordshire.gov.uk or see their website: http://www.hertfordshire.gov.uk/hals

Hertfordshire Archives and Local Studies (HALS)
Register Office Block (CHR002), County Hall
Hertford SG13 8EJ
0300 1234049

In addition HCC's Record Management Service provides a chargeable secure record storage and retrieval service for items not ready for archiving.

For more information, email rms@hertfordshire.gov.uk

Documenting of all Archiving, Destruction, Deletion and Digitisation of Records

To satisfy audit, accountability, legal and business needs, it is vital to keep a record of all archiving, destruction, deletion and digitisation. The Freedom of Information Act 2000 requires schools and Academies to maintain a list of records which have been destroyed and a record of who authorised their destruction. The Act states that, as a minimum, the school should be able to provide evidence that the destruction of records took place as part of a routine records management process. Schools must assess whether they are creating another piece of Personal Identifiable Information (PII) by maintaining a record of evidence, particularly if they are listing the names of the people whose records have been deleted.

A comprehensive records management policy and retention schedule will provide a detailed process to ultimately ensure that the records have been destroyed and should stand as the minimum required under the FOI Act.

A record should be retained of:

- File reference (or another unique identifier)
- File title (or brief description)
- Number of files or volumes
- Date range
- Reference to the applicable retention period
- The name of the authorising officer
- Date approved for disposal
- Date destroyed or deleted from system
- Method of disposal
- Place of disposal (whether on-site or off site by a contractor)
- Person(s) who undertook destruction

Management & Monitoring of Electronic Communications

Introduction

These guidelines have been developed to provide information about electronic communications best practice, and will hopefully help you balance staff and student privacy with the oversight necessary to ensure your safeguarding obligations are maintained.

All electronic communications, whilst they are held, are disclosable under Freedom of Information and Data Protection legislation. Be aware that anything staff write in an email, an Instant Message (IM), a text, or on a message board, could potentially be made public.

Electronic communications are very easy to copy and transmit and although you may have deleted your copy the recipients may not. Because of this they can form part of your records, commit you to contracts and expose the school to risk if used badly.

Email

Watch your language

As communicating by email is quick and easy, the language in which email is written is often less formal and more open to misinterpretation. Use spell-check and consider the tone of the wording. Limit references to other people, and ensure that only factual statements, and no personal comments, are recorded.

Choose your recipients

Check the recipients are appropriate and typed correctly. Consider using role-based shared mailboxes (e.g. senco@ schoolname.region.sch.uk / head@academy.org.uk), ensuring you can control who has access to any accounts.

Consider turning off the 'auto-complete' feature in the 'To' box as staff could easily send an email to the wrong address.

Ensure that Bcc is used where appropriate to avoid the unauthorised disclosure of email addresses of intended recipients. (Note: the ICO has taken enforcement action in cases where Bcc has not been used in sensitive cases.)

Secure your data

The consequences of an email containing sensitive information being sent to an unauthorised person could result in sanctions or even a fine from the Information Commissioner, along with adverse publicity for the school. Confidential or sensitive information should be sent by a secure encrypted email or data transfer system. **Never put personal information (such as a pupil's name) in the subject line of an email.**

Secure your devices

If staff are allowed to use their own devices to access email, be aware that Outlook will download the entire contents of a person's mailbox onto the device. The school's IT support provider should be contacted for help with configuring personal devices and to check for encryption, as well as ensuring that all devices require a suitable password for access. You could advise staff to only access work email via the internet as the web client does not save data locally.

It is not a filing system

Email systems are commonly used to store information which should be stored somewhere else. Emails and attachments should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Where the text of the email adds to the context or value of the attached documents it may be necessary to keep the whole email. The best way to do this, and retain information which makes up the audit trail, is to save the email in .msg format. Where you just want recipients to read a document, consider sending a link to the documents rather than attaching them.

How long do we keep emails?

Email is a communications tool, and email applications are not designed for keeping email as a record. Email that needs to be kept should be identified by content, for example:

Does it form part of a pupil record?
Is it part of a contract?
Does it relate to an employee?

The retention for keeping these emails will then correspond with the types of records found in the Retention Schedule for schools below. These emails may need to be saved into an appropriate electronic filing system or printed out and placed on paper files. Similarly, information contained within these emails should be recorded in the appropriate place (e.g. the MIS). Once this is done the original could be deleted.

The school may wish to consider implementing an electronic rule whereby emails in inboxes are automatically deleted after a period of time, assuming they have been filed away. This will assist greatly in reducing the amount of information potentially disclosable in the event that a subject access request is received. You should also ensure that you have procedures for the management of accounts of staff who have left the organisation.

Do you want a disclaimer?

Adding a disclaimer to an email can mitigate risk, such as sending information to the wrong recipient. Typically, disclaimers cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and that any views or opinions of the sender are not necessarily those of the school. However, legally it is likely that these are not enforceable, but at the very least they can help clarify the school's position in relation to the information being emailed.

Look out for Phishing!

Make sure staff are aware of the dangers of providing information over email. Never provide passwords or personal data, or click on a link in an email without verifying its source. Ask your IT department to provide advice.

Messaging: Texts, Instant Messaging

Text messaging and IM applications can provide a quick, efficient way of communicating with individuals or groups. These methods are largely suited to brief, informal messages; more formal conversations may be better suited to email, telephone or delivered face-to-face. Avoid sending and posting sensitive/personal data as these systems may not be as secure as email.

Consider your audience – it may be necessary for a message to be sent to an individual or a group of people but bear in mind that not everyone may have access to these tools and may not have given permission for their contact details to be used in this way. It may also create privacy issues if third parties are able to read messages not intended for them.

Internal Discussion Boards and Forums

Internal discussion boards and forums (e.g. Intranets, Microsoft Teams etc.) provide flexibility for collaboration in the workplace. They can also be very informal and are essentially public within the organisation, although some functionality can be shared with external parties and because of this they should never be used to share confidential or personal information.

Always ensure that staff or students that use these groups and spaces are aware of exactly who will see any information posted.

Any recorded information is subject to the same Data Protection and Freedom of Information legislation, regardless of format, therefore it would be advisable to only use these methods

of communication to transmit information which you would be content to publish, that is to say; low risk information due to the lack of effective security and assurance.

Records Management

Content created and shared by messaging and discussion forums should be regarded as ephemeral and temporary. If the content subsequently becomes important (and is something that needs to be retained as a formal record, for example in a safeguarding case file), then it should be copied and moved into your filing system, either by saving it in a readable electronic format, printing it out or taking a screenshot. Whilst content does exist though, it is subject to both FOI and DPA.

Monitoring Staff and Student Use

Monitoring student and staff use of communications and the internet is a balance between a school's Safeguarding and PREVENT obligations and the user's right to privacy. It will be important to include this in the appropriate policy so you can demonstrate what you intend to do and to justify this in relation to your legal obligations.

An employer can monitor the use and content of staff communications provided it has informed members of staff that it may do so. If you intend to do this you will need to be able to prove that you have made staff aware that this may happen. You will need to provide staff with advice on how you expect them to use systems such as email, telephone, other messaging systems and the Internet (including Social Media). Ensure you make a decision about how your IT provider logs people's use of your email and internet, that the logging is an appropriate record, and that it suits your policy.

Where third party support has access to logs (remote support purposes, etc.) then you need to establish how long they, as a data processor, retain any information which may contain personal information. You should instruct the third party about the retention period based on the school's requirements.

The Information Commissioner's Employment Practices Code is an excellent resource to use when considering this area:
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

What You Need to Know About Social Media

Social Media can be used as a multi-use communication tool

Social Media forms a range of versatile tools that can be used in several ways. As a communication tool it can broadcast information, enabling a quick way to share information about the school in the form of text, pictures, video and/or audio. It can be used to have direct communications with stakeholders on a one-to-one, one-to-many or many-to-many basis, or it can make use of provided information to see who the school is engaging with.

The school must ensure that staff contributors maintain the school's standards for written communications on Social Media platforms. Changes to Social Media tools are fast-paced and so it is not always possible to give consistent instructions for certain tasks. There are several organisations that can support you with understanding how to set up and make the most of Social Media tools, usually with a strong emphasis on the role safeguarding plays with these tools.

Use of Social Media may require a risk assessment prior to implementing Social Media, as staff must think about information security when they are sending or replying to messages/posts. Use of Social Media should follow protocols and procedures established

by the school to ensure consistent use of Social Media and that staff do not release information inappropriately or illegally.

Schools using social media will need to establish what purpose they are using it for, the lawful basis as part of it, what data/information they will process, how they will uphold any of the rights of data subjects, and the retention periods involved. This is usually completed as part of a Data Protection Impact Assessment. Depending on how the school is planning to use Social Media tools, it may opt to complete an assessment, one per tool or bring several together based on how data flows through them (e.g. a blog post which may be tweeted and then finally published on Facebook, but is actually part of a single data flow).

Social Media is not always a secure and private platform

Social Media tools have a range of settings for both security and access to published posts/comments. This needs to be taken into consideration when publishing information and controlling who has access to it. Confidential or sensitive information should never be put online or shared via direct contact on Social Media. Where images, names of individuals or other personal data is used schools must ensure that they have a lawful basis for doing so.

Where this involves consent from the parents/children, the consent should be clear and unambiguous, including where the information will be shared and for how long. Records of consent should be kept with other records for the individuals involved where possible, but access must be provided for those that require it as part of day-to-day operations. It is important for parents and students to understand that, when giving their consent, the school cannot control the re-posting of information.

See also: https://www.saferinternet.org.uk/advice-centre/social-media-guides.

Social Media posts vary in their retention

Social Media tools vary in their retention periods. When signing up for any tool the school needs to ensure that users are aware of these retention periods and ensure that it checks on a regular basis for changes. Where the retention period is longer than that set out as part of standard school policies, processes must be in place to remove any posts or comments, or to publish this fact within the Retention Schedule. Where posts include items which are hard to clearly index/search (e.g. images, video or audio), then a content register may be needed to manage when items have been shared, when they were shared, who it was in reference to, etc.

Social Media posts and messages don't necessarily delete immediately

Posts and messages can remain on the Social Media network for a period after the school has deleted them. Once messages have been posted they may be shared, liked and commented on (in ways not originally intended). If so, there will still be copies in existence and if the recipient saves an image/screenshot they will have copies that can be distributed. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 2018 – they will also form part of the child or subject's digital footprint - clear and unambiguous consent is therefore key.

Social Media is disclosable under the access to information regimes

Both the Freedom of Information Act 2000 and Data Protection Act 2018 provide regimes for access to information based on specific requests. When completing risk assessments for publishing personal data this must be considered as part of enabling the rights of data subjects. FOI legislation also mandates that anything published as publicly accessible is potentially disclosable (subject to exemptions), either at the time or as part of any request.

Do staff and governors need another account for work?

In the same manner that using personal email accounts for work means that they will be subject to FOI requests, the same applies for Social Media accounts. It is recommended, on safeguarding grounds, that dedicated work accounts are used and managed by the school. Any official school account should be tied to school email addresses, and ensure that there is transparency within the school on who has access to these accounts.

Creating and sending messages/posts

Here are some steps to consider when sending messages and posting:
Do you need to send this message/post?
Do you need to communicate via Social Media, or would it be more appropriate to telephone or speak with someone face-to-face?
Ensure that the messages/posts are clearly written.
Do not use text language or informal language in school messages/posts.
Always sign off with a name (and school contact details - never personal details).
Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.

Never write whole messages/posts in capital letters as this can be interpreted as shouting.
Always spell check messages/posts before you send them.

Sending attachments

Sending attachments on Social Media should be avoided; you should not be sending content to parents etc. via this platform. If they want to receive content, then they should make a request in person at the school or via authorised means for it to be processed. This ensures that compliance with data protection legislation is followed, as well as ensuring safeguarding issues are considered.