Llywodraeth Cymru
Welsh Government

GUIDANCE

Guidance for schools to implement the information management strategy

Help for schools to apply the information management strategy and data protection recommendations.

First published: 6 August 2021

Last updated: 20 March 2023

Contents

Data protection and school administration

In the collection, storage and processing of personal information regarding pupils, the school is acting as 'data controller'. This means that the school must satisfy certain obligations in order to comply with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). Pupils and staff, being the subject of the data held, are 'data subjects' and as such have rights, protected by the act, with regard to the data held about them.

Under the Data Protection (Charges and Information) Regulations 2018, schools as 'data controller' must register with the Information Commissioner's Office (ICO) and pay a data protection fee unless, you are exempt. You must adhere to UK GDPR requirements.

Registration with the ICO must be renewed annually, via an online application form. When any part of your entry on the ICO's register of data controllers becomes inaccurate or incomplete, you must inform them. This action must be taken as soon as practicable. More information is available from the **ICO**.

Most data controllers will need to inform the ICO, in broad terms, of the purposes of their processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register.

The school must:

- issue a privacy notice (sometimes known as a fair processing notice)
- set out in the privacy notice what data is collected, how it is used, how long the data is kept for and with whom it is shared
- issue the privacy notice to every new pupil who joins your school
- either update the existing privacy notice, or issue an additional privacy notice, whenever any changes are made to data collections and/or data

sharing arrangements

The **Welsh Government's privacy notice for the statutory collections of pupil data is available**. Schools and local authorities may wish to refer to this to support their own privacy notice requirements, but must issue their own school level and local authority level privacy notices. Further guidance is available from the **ICO**.

Schools should also:

- ensure the data that is collected, stored and/or processed on all pupils and staff is effectively and efficiently maintained so that it is as accurate and up to date as is reasonably possible
- ensure the **security** of their data and the systems used to store and access it
- respect the rights of individuals in relation to the data held on them, including responding appropriately to requests for access to personal records
- take all reasonable action to ensure that pupils, and where appropriate their parents, are aware of their **rights in relation to personal data** held on them
- put in place information sharing protocols, where necessary, setting out the conditions under which they provide information to others

The UK General Data Protection Regulation (UK GDPR)

The processing of information that relates to an identified or identifiable individual (personal data) is governed by the UK GDPR. Those who decide how and why personal data are processed (data controllers), and those who may carry out the processing on behalf of controllers (data processors) must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the UK GDPR.

UK GDPR puts the onus of compliance on the data controller, whereas there are

more limited compliance responsibilities placed on the data processor. In the collection, storage and processing of personal data regarding pupils the school is acting as a data controller. This means that the school must comply with the UK GDPR when it processes pupil personal data.

Article 5 of UK GDPR sets out the principles relating to the processing of personal data. These include ensuring that:

- the legal basis for processing has been identified
- pupils are informed about how their personal data will be used by issuing a privacy notice to every new pupil who joins the school
- appropriate **security arrangements** are in place in terms of the systems and processes used to store personal data and access it

Pupil rights

The UK GDPR gives all individuals, regardless of age, the general right to find out what data is held about themselves by any 'data controller' on computer and most paper records. Requests to see or receive copies of records are known as 'subject access requests' and should generally be made in writing to head teachers.

If an individual is incapable of understanding or exercising their own rights under UK GDPR, for instance because they are too young, parents or legal guardians may make subject access requests on their behalf.

" Remember, there is no automatic right for a parent or legal guardian to have access to data held on children in their care. Further, there is no mandatory age limit set for when a pupil may be deemed too young to understand, and therefore exercise their rights. However, the presumption is that, by the age of 12, a child may have sufficient maturity to understand their rights and to make an access request themselves if they wish. Each

> case or request should be considered on its own merits. "

The rules of good information handling: the principles

Anyone processing personal data must comply with the eight enforceable principles of good practices. They say that data must be:

1. fairly and lawfully processed
2. processed for limited purposes and not in any manner incompatible with those purposes
3. adequate, relevant and not excessive
4. accurate
5. not kept for longer than is necessary
6. processed in line with the data subject's rights
7. secure
8. not transferred to countries without adequate protection

Personal data covers both facts and opinions about the individual. It also includes information regarding the intensions of the data controller towards the individual.

Processing personal data

'Processing' is broadly defined and takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed "fairly and lawfully". A data subject must be told the identity of the data controller and why that information is to be processed; these details are given in a 'Privacy Notice'.

Processing may only be carried out where at least one of the following

conditions has been met:

- the individual has given his or her explicit consent to the processing
- the processing is necessary for the performance of a contract with the individual
- the processing is required under legal obligation
- the processing is necessary to protect the vital interests of the individual
- the processing in necessary to carry out public functions
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual)

Special Category data is personal data that needs more protection because it is sensitive. In order to lawfully process special category data, you must identify one of the conditions above and a separate condition for processing under Article 9. For further details please refer to the ICO website on **GDPR and Special Category data**.

Security

Data controllers must take security measures to safeguard personal data. UK GDPR requires that data controllers must take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of data. Where a controller uses the services of the data processor the security arrangement must be part of a written agreement between the two.

The rights of individuals

1. The right to be informed

UK GDPR allows Individuals to be informed about the collection and use of their personal data.

2. The right of subject access

UK GDPR allows individuals to find out what information is held about themselves on computer and some paper records. Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly known as 'subject access request' (SAR).

3. The rights of rectification, erasure and destruction

UK GDPR allows individuals to apply to the court to order a data controller to rectify, erase, or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

4. The rights to restrict processing and object

Individuals have the right to request the restriction or suppression of their personal data. An individual can ask a data controller to restrict/suppress/stop or request that they do not process information relating to them where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.

5. The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

6. The rights in relation to automated decision making, including profiling

UK GDPR allows individuals the right to prevent decisions made without being involved, which is known as 'automated individual decision-making and profiling' or 'automated processing', for short.

The above notes are based on extracts from guidance on the **ICO website**. They are intended for information purposes only and should not be assumed to cover all aspects of the DPA 2018 and UK GDPR. Further advice is available from your local authority Data Protection Officer or by contacting the ICO at **wales@ico.org.uk**.

Keeping people informed

When schools collect, store and use personal data they have an obligation to inform parents and pupils through the issue of a privacy notice. Beyond this obligation, there are a host of ways that can be used to make sure that everyone knows and understands what the school is doing with their information, why and what rights individuals have.

Letters to parents and pupils

Schools may wish to use covering letters when sending out privacy notices or write separately to ensure that both pupils and parents are aware of their rights in relation to information that the school holds. Communications from schools may be hard copy or electronic.

Remember it is the pupil who has rights under the DPA 2018 and UK GDPR. The presumption is that, by the age of 12, a child has sufficient maturity to understand their rights and to make an access request themselves if they wish. In certain circumstances, depending on capacity to understand, a parent or legal guardian may seek to exercise some of these rights on behalf of the pupil. In such circumstances, the school must decide whether it is appropriate to act on the request. A parent would normally be expected to make a request on a child's behalf if the child is younger.

School websites

A copy of the school's privacy notice should be placed on the school website, along with summary information and copies of letters sent to pupils and parents.

Schools may also find it helpful to include a link to the **Data management information: privacy notice** and the **ICO website**, so that users can easily access further detailed information if they want to.

Statement on forms

Schools often use forms, for new admissions, checking information and contact details. Where forms are used for collecting or checking personal data, schools may wish to include wording similar to the following:

> " The data requested will be stored on the school management information system and used for the purposes outlined in our privacy notice. Every effort is made to ensure the accuracy and security of personal data held by the school. Individuals have certain rights of access to personal information that local authorities and the Welsh Government hold about them. "

The addition of such a statement to data collection and checking forms is considered to be best practice by the Information Commissioner's Office.

Please note, however, that the addition of this statement to data collection forms does not negate the need to ensure that every parent or pupil receives a copy of the privacy notice on first entry to your school.

Statement in school prospectus and governors' annual reports

A statement could be added to the school prospectus and/or governors' annual report to parents along the lines of:

> " The school collects information about pupils and their parents or guardians at admission to school and for specific purposes during the school year. Every effort is made to ensure the accuracy and security of the data collected which is generally stored on the school's computerised management information system. Individuals have certain rights of access to personal information that local authorities and the Welsh Government hold about them. "

Again, use of this text in your prospectus or governor's report will not negate the need to issue copies of the privacy notice. It should be noted that the addition of this statement is NOT a statutory requirement under the school prospectus or governors' annual report regulations.

Schools may also consider including the full text of the privacy notice in the school prospectus, however care must be taken to ensure that every pupil (or their parents) joining the school receives a copy.

Information security for schools

Schools have a duty to protect the information they hold, particularly data about people.

Information security is about maintaining:

- confidentiality: ensuring only people who have a right to see the information can actually do so
- integrity: making sure the information is right
- availability: making sure that the information can be accessed when required

Schools record a range of detailed information to support their statutory duties and day-to-day activities. Information security is, therefore, essential. Poor security can lead to:

- not being able to do your job
- not being able to meet important deadlines
- frustration for other school staff
- embarrassment for the school
- legal challenges

Security cannot be completely watertight. It is important to choose security measures that suit the school's own circumstances. It is wise to consider the risks, threats and vulnerabilities that apply to your school and choose appropriate security measures to counter them. Information security is for everyone in the school. Good security brings benefits to everyone and should be practised by everyone. The rules that apply in the school also apply to equipment and hard copy or electronic documentation used for home working.

Personal data

The UK General Data Protection Regulation (UK GDPR) sets out requirements for how organisations, including schools, need to handle personal data (please see the **ICO website** for further information). Personal data is defined under the UK GDPR as 'any information directly or indirectly relating to an identified or identifiable individual'.

Information about identifiable individuals is personal data. Personal data is data

that relate to a living individual who can be identified:

- from the data
- from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller

Personal data also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The UK GDPR also refers to the 'special categories of personal data'. This means personal data about an individual's:

- race
- ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data (where this is used for identification purposes)
- health data
- sex life
- sexual orientation

Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

The precautions that should be taken are applicable irrespective of media type. For example, each of the following can require security measures if they contain personal data:

- emails
- photos

- electronic documents
- handwritten notes

The **HM Government security classification policy** has three categories (Official, Secret and Top Secret). Information processed within the school environment will fall into the Official category defined as:

> " The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. "

For Official data the information security outcomes should:

- protect against deliberate compromise by automated or opportunistic attack
- aim to detect actual or attempted compromise and respond

Hwb

Hwb is the centrally-funded, digital learning platform intended for providing access to a range of digital content and tools. It has been designed primarily to store educational content that can be shared with any other Hwb user. Although access to the Hwb platform is only available to registered Hwb users, it is not intended to store sensitive data. Where schools are required to handle sensitive data, this should be done via HwbCloud. Further information on Hwb, and HwbCloud security can be found via the **Hwb trust centre**.

Protecting equipment

The following are examples of precautions that could be taken but are not

exhaustive. Schools should also refer to locally agreed policies.

- consider the placement of computers (for example ensuring that screens cannot be seen from windows or corridors)
- fit locks on doors, cupboards and computers to make theft difficult; remember to set locks and alarms
- keep keys, combinations and passwords securely; they should be just as secure as the equipment and information they protect
- seek and apply the advice of the local crime prevention officer and local authority information security experts
- place computers and cables where they won't be a hazard (for example don't run cables across walkways)
- arrange for repairs to equipment to be carried out by appropriately qualified personnel only
- place computers away from sources of heat, water and chemicals to avoid damage
- keep an inventory of equipment, software and data so that you can quickly identify what's missing if you suffer theft or fire; it is wise to keep a copy of the inventories off site: securely of course
- always report concerns about inappropriate usage: local procedures should be followed as necessary
- take special care of easily portable equipment (for example a laptop computer), as it is easy to steal; equipment is particularly vulnerable if left on display in cars
- the use of personal devices will almost certainly introduce risks to the information processed on them; this is each school's risk management decision

Protecting information

- ensure that everyone who uses a computer system is properly set up to access only the information they need and has a logon ID and password

- keep passwords strictly private: there should be no need for anyone else to know users' passwords; do not share passwords
- be discrete when using information, especially information about people
- if you are contacted by telephone, you must ensure you are aware of the identity of the caller before discussing official business; this is particularly important should you be discussing information that is sensitive
- safeguard information held electronically and on paper equally well; use passwords to protect sensitive files and restrict access to authorised users (if keys or passwords are easily found, the information they are meant to protect isn't really secure at all)
- double-check email addresses and phone numbers are correct before sending information to make sure it isn't sent to the wrong person
- use only approved and authorised software
- avoid use of public, shared or personal devices or systems for sensitive or personal data
- all staff should be properly trained before using information systems
- check the data that you put into, and get out of, information systems: your decisions can only be as good as the information you use
- log off or lock the computer before leaving it, even if only for a short time
- put paper information away
- make regular backups of data and test that they can be restored
- store backups and original copies of software away from computers, preferably in a fireproof safe
- publicise this guidance and the school's security policy
- don't allow your data to grow beyond the school's needs: archive old data that's no longer needed; alternatively, monitor your system's use of storage and buy more before it is needed
- ensure that no one can access information unless they are authorised
- arrange for visitors to be accompanied and supervised, especially if they need access to the school's information
- the practice of taking sensitive documents off the premises to be worked on at home or on the way to an official meeting should be discouraged since it

increases the risk of compromise; the same applies to access to such material in home working posts

- if transferring personal or sensitive information via email, consideration needs to be given to ensure the information is sent securely (ideally encrypt the email before sending)
- try not to use mobile phones to discuss sensitive information. Calls made on mobile phones are insecure and may be overheard by someone who should not hear this information

Special problems: computer viruses and cyber attacks

- ensure that all the school's computers are protected by anti-virus software and that it is kept up to date
- ensure that all the school's computers are using web browsers that are up to date and are kept up to date
- regularly scanning computer with an antivirus software is one of the easiest and best ways to prevention of computer virus attack and removing infections
- avoid using media from high risk sources: for example, from the internet, people you don't know or people who don't have proper anti-virus measures
- avoid downloading software from the internet where possible unless you know who it from, as this can allow spyware and network sniffing software to also be downloaded
- be aware that hoax virus alert and phishing scam emails can lead to as much disruption as real viruses; do not act on email warnings and instructions unless you are certain they come from a reputable expert
- if in doubt, do not click on it and seek expert help
- best practice recommends that updates are made to computer operating systems on a regular basis with the latest security patches, in order to protect from computer virus attacks and malware
- only download software and apps from trusted sites or sources

If you think you have a computer virus

- don't panic: if you have up to date anti-virus software it's unlikely that your system will have been infected
- if the infection has been detected on your PC, close it down as you normally do (don't just switch it off) and seek expert help

More information on cyber attacks and advice for schools is available from the **National Cyber Security Centre**.

Legal requirements

There are a number of laws that regulate the ways in which information is used, especially where the information is about people. These include the:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018; this sets out how personal data may be obtained and processed lawfully (separate advice for schools is available)
- Freedom of Information Act 2000; this provides a public "right of access" to information held by public authorities
- Computer Misuse Act 1990; this is the main anti-hacking law, which makes unauthorised use illegal, including unauthorised use by employees
- Copyright, Designs and Patents Act 1988; this treats computer software as copyright material and thus makes copying programs without the appropriate license illegal
- Health and Safety at Work Act 1992; this is intended to make workplaces safe; separate regulations (the Display Screen Equipment Regulations) set out the proper conditions for using computers

Retention of school information

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use, as well as the basis for normal processing under the DPA 2018, UK GDPR and the Freedom of Information Act 2000.

There are a number of benefits which arise from the use of a complete retention schedule:

- managing records against the retention schedule is deemed to be "normal processing" under the DPA 2018, UK GDPR and the Freedom of Information Act 2000; provided members of staff are managing record series using the retention schedule, they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a data subject access requests have been made
- members of staff can be confident about shredding information at the appropriate time
- information which is subject to freedom of information and data protection legislation will be available when required
- the school is not maintaining and storing information unnecessarily

Safe destruction or preservation of records

Where records have been identified for destruction, they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information should be shredded before disposal using a cross cut shredder. Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in

the dustbin or a skip unless there is no other alternative. There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- file reference (or other unique identifier)
- file title (or brief description)
- number of files
- the name of the authorising officer
- date action taken

This could be kept in an Excel spreadsheet or other database format.

Transfer of records to the archives

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the school archives.

Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to electronic records. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Further information on the keeping, disposal, disclosure and transfer of pupil information can be found in the Welsh Government guidance on **educational records**. A sample of a retention schedule can be found at Annex A of this guidance.

Unique pupil number

The unique pupil number (UPN) is a number that identifies each pupil in Wales uniquely. A UPN is allocated to each pupil according to a nationally specified formula on first entry to school, and is intended to remain with the pupil throughout their school career, regardless of any change in school, local authority or even where they move between schools in Wales and England.

The scope of the UPN system is the maintained schools sector. This includes maintained special schools, pupil referral units and nursery schools. Every pupil in a maintained school in Wales should be issued with a UPN on their first entry to school.

The UPN is, as far as possible, a blind number held by schools on the pupil's electronic record, and only output in specific circumstances. It should not be regarded as an automatic adjunct to the pupil's name, routinely appearing on any paper record or documents relating to them. It is particularly important that the UPN is closely guarded as it relates to an individual and should, therefore, not be widely and openly displayed in a manner that could compromise its confidentiality.

For UK GDPR purposes, the UPN is considered personal data and, as such, UPNs held with or without other data items remain within the scope of UK GDPR and must be **protected accordingly**. Schools and local authorities have a responsibility for maintaining the privacy of individuals about whom they collect, process or hold personal data and it is for schools and local authorities to be satisfied that their use of personal data is lawful and compliant with the DPA 2018 and UK GDPR.

Implications for schools on the use of the UPN

Schools should not generally advise pupils or parents of their UPN, nor take any positive steps to inform them of the existence of the UPN. Schools will of course wish to deal with any enquiries from pupils or parents honestly and without evasion, and pupils have the right, under the UK GDPR to receive on request a copy of any information the school holds about them. However, reflecting the Information Commissioner's Office's (ICO) view that the UPN is an identifier for use solely in the educational context, particular care should be taken to prevent potential abuse of the UPN outside of its use in education. Thus, schools should not give out details of pupils' UPNs, other than as a result of a lawful and legitimate request.

Schools should not enter UPNs on pupils' paper files or on any other physical documents, including admission and attendance registers, and should continue to use the admission number, not the UPN, as a general pupil reference number within the school. Schools should store pupils' UPNs in their Management Information System (MIS) using educational software packages. Storing UPNs electronically will minimise security risks and adhere to UK GDPR requirements.

Schools are advised that, generally, the UPN should not appear in printed format. In the event that this does happen then the printed document should be kept securely and shredded immediately, to prevent inappropriate use or a breach of security.

Use of UPNs by other local agencies

The use of UPNs is restricted to education related purposes only. This imposes some limits on the extent to which other local agencies may have access to pupils' UPNs.

Under the guidance provided by the ICO, UPNs should not be used as a replacement for pupil identification systems already in place in local non-educational departments. Local agencies should, therefore, continue to use local identification systems, as use of the UPN as a replacement identification system could undermine the commissioner's wishes that UPNs are not widely and openly displayed in a manner that could compromise their confidentiality.

It should be noted that, in the case of looked-after children, regulations now permit the transfer of individual pupil data to the social service department of the local authority which looks after the relevant child or children whose data are being transferred, to help in ensuring that these children receive appropriate educational provision, and that their progress is monitored both individually and as a group. It would be legitimate to use UPNs to facilitate this exchange of information, but not for social services departments to go on from there to adopt UPNs as a general client identifier used for their own purposes, whether education related or not.

Sharing UPNs with third parties

Where a school or local authority has entered into a contractual agreement with a third party supplier, it is permissible for the UPN to be used within that system, provided that:

- the use of UPNs, rather than any other identifiers, is necessary for the provision of the service and compliant with ICO guidance
- in entering into an agreement with a third party, the school or local authority retains control and ownership of the data
- the third party is aware of its own data protection and UK GDPR, with respect to data processing
- the service being provided is solely for education purposes
- schools and local authorities satisfy themselves that, in agreeing to share UPNs, they remain UK GDPR compliant

Examples of such third party arrangements include the provision of school MIS and additional packages supporting schools with the management of a pupil's education. In such cases, the third party would be classed as a data processor on behalf of the school, for data protection purposes.

The sharing of UPN data with a third party for work or service not commissioned by the school or local authority would not be permitted, nor would sharing of the UPN for any purposes not related to education.

Issuing UPNs

Under the national formula UPNs have 13 characters as follows:

- character 1: a "check letter" derived according to a specified formula from characters 2 to 13 (enabling mis-reporting of the UPN to be detected, since if any of characters 2 to 13 are reported incorrectly the check letter at character 1 will not tally)
- characters 2 to 4: the local authority code of the school allocating the UPN (at the time that it does so)
- characters 5 to 8: the Welsh Government (WG) number of the school allocating the UPN (at the time that it does so)
- characters 9 to 10: the academic year in which the UPN is being allocated (i.e. the calendar year in which that academic year commences)
- characters 11 to 13: a serial number for UPNs allocated by that school in that year

The motivation for including the local authority code, WG school number and year of allocation in the UPN is to provide an effective and operationally simple means of guaranteeing uniqueness (ensuring that two schools cannot by chance allocate the same number to two different pupils).

This formula relates to permanent UPNs. There are also temporary UPNs,

allocated when a school receives a pupil who is likely already to have a UPN, but the school is not told what that UPN is. The formula for temporary UPNs is identical to that for permanent UPNs, except that characters 11 to 13 are a two digit serial number plus a letter (rather than a three-digit serial number).

All software suppliers of standard school MIS software known to the Welsh Government have incorporated into their management information systems, functions to automatically allocate permanent UPNs to pupils, and (where required) temporary UPNs.

The situation in Scotland

Schools in Scotland are not required to allocate UPNs, but some schools may do so. However, UPNs issued by schools in Scotland should not be used, because local authority numbers used in Scotland overlap with those in England and Wales and this may lead to duplication of UPNs. A new permanent UPN should be allocated to pupils transferring from Scotland.

When UPNs should be allocated

All pupils in maintained settings, including standalone nursery schools and nursery classes, must have a UPN allocated. Every pupil included in the Pupil Level Annual School Census (PLASC) return must have a UPN allocated.

UPNs should be allocated on pupils' first entry to a maintained school, including entry to a nursery class in an infant or primary school, and including entry to a standalone nursery school.

It follows that nursery, infant, primary or special schools will allocate the vast majority of UPNs. Secondary schools should only need to allocate UPNs to pupils who enter the maintained sector at age 11 or later, having spent the

whole of their school career up to that point outside of Wales or England or in the independent school sector or being electively educated at home.

What to do when a pupil transfers to your school

When children transfer from one school to another, it is important that the 'new' school has, and is able to act on, information about them.

It is essential, in order to maintain the integrity of the UPN system, that the transfer of UPNs with pupils from school to school is as complete and accurate as possible. Maintained schools should make reasonable and collaborative arrangements to obtain a pupil's previously issued UPN.

Pupils transferring to the school from another maintained school in Wales or England should be assumed to already have a UPN. The previous UPN should be sought and used by the new school.

Pupils transferring to the school from a non-maintained school or from Scotland, Northern Ireland, or outside of the UK are unlikely to have a UPN and, therefore, a new UPN will need to be created for them. Where it is thought that a pupil may have previously been educated in a maintained school in England or Wales, their old UPN should be reassigned to them. A new UPN should only be created if the school has been unsuccessful, after reasonable efforts, in locating the pupil's previously issued UPN.

Local authorities are encouraged to act as 'clearing houses' for pupil records, certainly for the main primary to secondary transfer: receiving records from primary schools and distributing them to secondary schools. This is likely to be more efficient than direct school to school transfer (given the many different pathways pupils may take between the primary and secondary schools in an area). It will also be more robust in relation both to the transfer of pupil records as a whole and of UPNs in particular, and provides the local authority with

important information for its own purposes. Most local authorities operate systems of this kind.

When to issue temporary UPNs

In the event of being unable to trace a previously allocated UPN, a school may need to allocate a temporary number for interim use. This will be necessary if the school needs to compile their PLASC return while the pupil is on roll. PLASC returns cannot be completed without a valid UPN.

If, after a temporary UPN has been allocated, an earlier UPN for the pupil is retrieved, then the school should replace the temporary UPN that it initially allocated with the previous UPN (even if that is itself a temporary number). If all reasonable attempts to trace a previously allocated UPN have been unsuccessful, the temporary UPN should be converted to a permanent one.

If a pupil arrives at a new school without a **common transfer file (CTF)**, this should be requested from the old school, rather than entering pupil information manually into their MIS and generating a new UPN unnecessarily.

UPN and adopted children

Pupils who are adopted after they have been allocated a UPN should be issued with a new permanent UPN. Their previous UPN should be deleted and not recorded under 'former UPN'. As part of this process, it is important that there is no link retained between the pre-adoption record (with the original UPN) and the post-adoption record (with the new UPN).

In situations where the adoption creates no safeguarding risks to the individual pupil (for example, where the child has remained within the same school before, and after, adoption and has undergone no material change in identity as a result

of the adoption), it is permissible to retain previous UPN information for the adopted pupil, where permission has been granted by both the pupil's adopted parents and the designated manager of the local authority's adoption service.

This advice will, however, always need some level of consideration for each individual case, in consultation with the local authority adoption services, to make sure it is right for their circumstances. It is for the local authorities involved to apply that level of consideration, rather than the Welsh Government.

Children at risk

Schools may receive pupils who, for their own safety, have changed their identity. This will be the case for children in the witness protection programme and for those fleeing from abusive family members. As part of their new identities, these pupils must be issued with new permanent UPNs and their previous UPN must be deleted and not recorded under 'former UPN'. As part of this process, it is important that there is no link retained between the original and new pupil records.

Troubleshooting

Invalid UPNs

When a school enters a UPN that it has received from a pupil's previous school (most UPNs are sent via the **common transfer system** as part of a CTF), the school's MIS software will check the validity of that UPN and inform the user if it is not a valid number. If the UPN is invalid, then the school should:

- check that the UPN has been recorded correctly, and, if it has been
- check that the previous school has provided the UPN accurately

In order to be valid, a UPN must:

- be 13 characters long
- have a recognised local authority (or 'pseudo local authority') code at characters 2 to 4
- have digits at characters 5 to 12
- have a digit or an upper case letter other than I, O or S at character 13
- have the correct upper case "check letter" at character 1 derived by a specified formula from characters 2 to 13

If it transpires that there has been no error in the transmission or recording of the UPN (i.e. that the UPN as held by the previous school was already invalid), then the receiving school should issue a new permanent UPN to the pupil. However, if it is believed that the pupil may already have been allocated with a valid UPN at some point in the past and this UPN has not been passed on, a temporary UPN should be issued only if a return is due, until the previous UPN has been traced. If the pupil has not already been allocated a valid UPN, a permanent UPN should be issued. Schools should report any changes to a child's UPN to their local authority.

Pupils not attached to any school

There are a number of groups of pupils unattached (either temporarily or permanently) to any maintained school in the local authority, but for whom the local authority has responsibility to ensure provision of an education. For example, permanently excluded pupils not yet assigned to a new school, home educated pupils and those educated outside of the mainstream school setting. (Pupils with special educational needs (SEN) who have a SEN statement or pupils with additional learning needs (ALN) who have an Individual Development Plan (IDP), but attend a maintained school in another area or a non-maintained school, are dealt with separately below.)

In cases where a pupil has previously been educated within the English or Welsh maintained system, but is currently permanently excluded or 'unattached' from a maintained school, the local authority should keep a secure record of that pupil's former UPN. If the pupil then re-joins a maintained school the local authority should forward this previous UPN to their new school.

Local authorities should only allocate a UPN to those pupils who have not previously been educated in the maintained system in England or Wales. In such cases, the pupil should be issued (using the appropriate UPN generating functionality in their MIS software) with a 'dummy' school number in the range 3950 to 3999.

It is essential, however, that the local authority has a single point of control for the allocation of UPNs to all types of pre-school or unattached pupil, to ensure that no two pupils are allocated the same UPN.

Dually registered pupils

It is essential that dually registered pupils be allocated only one UPN. Where a pupil is registered at two schools, one must be designated as their 'main' school, with this school only allocating them a UPN. The other 'subsidiary' school will then need to be notified of that UPN.

For PLASC purposes, where a pupil is dually registered between a mainstream school and pupil referral unit (PRU) or special school, both establishments should maintain a pupil record for the pupil. One establishment should record the pupil's registration status as 'main' and the other 'subsidiary'.

In deciding which establishment is 'main' or 'subsidiary' you should consider at which location the pupil is likely to spend the majority of their time during the academic year. For example:

- if a pupil spends a day a week at a special school or PRU then this should be their subsidiary establishment
- if a pupil is to attend a PRU full time for a limited period of perhaps a few weeks then return to the mainstream school the PRU would be the subsidiary establishment
- if a pupil is intended to spend over half of the academic year at the special school or PRU then records should show the special school or PRU as the main establishment

There may, however, be other forms of dual registration. For example:

- pupils registered at, and dividing their time between, two mainstream schools; in this case the pupil's 'main' school for UPN allocation purposes should be the one where they spend the greater proportion of their time
- pupils under 5 attending morning and afternoon nursery classes in separate infant or primary schools; it is suggested that the school they attend in the morning be deemed their 'main' school
- pupils from traveller families: special circumstances apply where a pupil 'has no fixed abode for the reason that their parent is engaged in a trade or business of such a nature as to require them to travel from place to place'; the pupil can be dual registered. In these cases, the school where the pupil has attended when the parent is not travelling during the preceding 18 months is their 'school of ordinary attendance'. In practical terms, this means the 'school of ordinary attendance' would record registration status as 'main'. Note that these pupils must also be recorded on the attendance register if they remain on the school admissions register
- post-16 pupils may be educated at more than one site, receiving part of their tuition at alternative locations through arrangement with their 'home' school; in such circumstances, the 'home' school is that which has responsibility for arranging a pupil's courses of study at any alternative location(s) and should be recorded as the 'main' school

Local authorities should notify the Welsh Government of other significant

incidents of dual registration, so that advice can be provided on handling. Please email **IMS@gov.wales**.

Pupils with SEN or ALN attending a non-maintained school or a maintained school in another area

A pupil with a SEN statement or an IDP maintained by the local authority who is:

- attending a maintained school in another area should be treated as that school's pupil for UPN purposes, and should be allocated their UPN by that school: with the local authority responsible for the pupil's SEN statement or IDP being notified of the UPN
- attending a non-maintained special school or independent school should be allocated their UPN by the local authority responsible for the pupil's SEN statement or IDP, with the school being notified of the UPN, so that it can be included when the school is reporting information about the pupil for (for example) assessment purposes

Your local authority will be able to give you further advice based on the specific arrangements that it has in place to support the use of UPNs. For technical queries relating to the software used in your school to issue and store UPNs, you should contact your usual support service.

Data Exchange Wales initiative (DEWi) and data collection

This section provides a high level description of the functionality within the DEWi system, together with an overview of the key data collection processes for which the system is used.

DEWi overview

DEWi is a secure online data transfer system developed by the Welsh Government (on behalf of Welsh Ministers) specifically to provide schools, local authorities and the Welsh Government with a means of exchanging electronic files easily and securely over the internet.

Since DEWi was launched in 2006, it has been through various stages of development and enhancement. Our aim is to enable statutory obligations to be met, whilst providing schools and local authorities with useful tools within an easy-to-use system.

Access to DEWi is only authorised for limited officials with a valid business need to use the system, in accordance with the intended use of the system. The use of DEWi and its user accounts is monitored regularly by the Welsh Government.

DEWi allows for the secure transfer and validation of pupil, workforce and school information for statutory data collections through a robust system. It provides a secure route for schools to share their data with their local authority, and in turn the Welsh Government. Tools are provided within DEWi to aid schools and local authorities to validate their data, prior to submitting their statutory returns to the Welsh Government.

DEWi is also used by the Welsh Government to share information with local authorities. It is not a tool for archiving data, which remains on DEWi for no longer than is necessary. DEWi is also not a transfer tool for files between schools or between local authorities.

DEWi can be accessed using a web browser application (for example Microsoft Edge, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox etc.).

On accessing the system, the sign in page will prompt users to enter a valid username and password. Once both of these are entered and validated by the system, the user will see the school, local authority or Welsh Government page, according to the user account's role and permissions.

Upload and validation of data collection files

DEWi allows schools and local authorities to upload statutory data collection return files that are output by their management information system (MIS) software, using specific file naming conventions, for the following statutory data collections:

- PLASC (Pupil Level Annual School Census)
- EOTAS (Educated Otherwise Than At School)
- NDC (National Data Collection)
- Attendance: Primary
- Attendance: Secondary
- Post-16
- SWAC (School Workforce Annual Census)

Files for the majority of the above collections, with the exception of EOTAS which is submitted by the local authority, are uploaded to DEWi by schools and validated by the system, according to the collection type. Validation looks at the format of the file, what data is present, and checks that the data conforms to defined sets of values. For the returns submitted by schools, local authorities will then access the system to assist in the resolution of any issues found in the files from their schools.

When any issues have been identified and resolved in the school MIS software, local authorities can request their schools to upload a revised file to DEWi which overwrites the original file. Once the data submitted is "clean", the local authority will submit the file to the Welsh Government.

Reports

A series of reports are available to schools, local authorities and the Welsh Government users for all data collections, which can be used for information and data validation purposes.

Downloads

Local authorities are able to download the data submitted by their schools as an XML file or set of CSV files, which may then be used for importing into their own software systems.

Administration

Email correspondence sent to schools from the Welsh Government regarding DEWi will be sent using those email addresses listed on DEWi, so it is important that schools check that their email address is recorded correctly in DEWi.

Passwords should be changed on a regular basis. Schools and local authorities can opt to change the password for their username at any point. Local authorities have additional functionality which allows them to reset the passwords for their school users.

Local authorities must remember that passwords issued by email must not contain the username for the profile in the same email. Username should be confirmed over the phone or by a separate email from the school. If the school has confirmed their username or school number in an email, then do not reply to the email, as their original message would be retained in the content.

Bilingual

DEWi is fully bilingual, with all screens available in both Welsh and English. The buttons displayed on the sign in screen will determine the initial language to be used when using the site. However, users can choose to change languages at any time on each screen viewed. All reports can be viewed in Welsh or English, irrespective of the language selected by the user for navigation through DEWi.

Overview of statutory data collections

Analysis of the individual pupil records, gathered through statutory data collections, provides schools, local authorities and central agencies with a range of information, which supports the drive to raise standards, the more accurate targeting of funding, and the monitoring and development of policy.

Data collected by the Welsh Government is published in the form of Statistical First Releases or **Bulletins** and on **StatsWales**.

The **key dates** for data collections and releases are published annually by the Welsh Government.

Pupil level annual school census (PLASC)

The **PLASC** is mandatory for all maintained schools (nursery, primary, secondary and special schools). All pupils on roll must be included in the PLASC return. PLASC is the key authoritative source of pupil and school level data on a wide range of areas from pupil numbers, free school meals and class sizes, as well as playing a key role in financial resource allocations, particularly through the Pupil Development Grant and the local government finance settlement. Data from this collection is used frequently and widely, both internally within the

Welsh Government and externally. PLASC data is published at a school level and, combined with data from the other collections, provides a valuable resource for the development, monitoring and evaluation of policy.

Educated otherwise than at school (EOTAS)

The **EOTAS** census covers pupils who are placed by local authorities in pupil referral units (PRUs) or other forms of alternative provision referred to as EOTAS. Most information is provided as individual pupil records. Each local authority is required to provide the Welsh Government with pupil level data for all pupils for whom the local authority has a responsibility to provide an education. That may take place in a PRU or in another form of alternative provision. The provision made for the pupil may be located within or outside the local authority area.

National data collection (NDC)

The **NDC** is an annual pupil level collection of statutory baseline and end of key stage (Foundation Phase, Key Stage 2 and Key Stage 3) teacher assessment data.

The data is published at a national level only. Local authorities and schools are able to use national level data in their self-evaluation, strategic planning and target setting practices. The data from this collection is also used by the Welsh Government for research and policy development and evaluation. For example, it will be used to understand how particular policies affect learner outcomes and to track national performance trends and the differences among groups of learners, such as those eligible for free school meals (FSM) and those with additional learning needs (ALN).

Attendance (primary and secondary)

The Welsh Government needs to collect **attendance** data on a regular basis to understand overall attendance patterns and to identify the characteristics of pupils who are not attending.

Analysis shows a relationship between attendance and attainment. Schools with high attendance levels tend to have high levels of attainment at all key stages, but those with low attendance levels tend to have low attainment levels. The attendance register is, therefore, an important tool in the work of schools to drive up standards and pupil's attainment. It helps them to identify pupils who might need extra support to catch up lessons they have missed along with action to tackle poor attendance.

The most effective way of minimising the adverse effect that absence has on a pupil's attainment is to prevent all unnecessary absence and, where the absence is unavoidable, to help children catch up the work that they have missed.

Post-16

All maintained secondary and middle schools that had pupils in the national curriculum Year 12 or above, at any time in the previous academic year, must submit a **post-16** collection return. The post-16 collection is a whole year data submission that uses learning programme and activity codes to identify the programmes, qualifications, subject and level of the learning activities undertaken in the previous academic year. It enables the Welsh Government to use the data to calculate the achievement measures, which include the retention and achievement of learners undertaking A level, vocational and Welsh Baccalaureate programmes.

The post-16 planning and funding framework was introduced with a key aim to better understand the return the Welsh Government gets from its investment in the post-16 sector in Wales. The framework aims to make better use of actual pupil current information to influence planning and funding decisions. The data is used to derive future years' local authority school sixth form funding allocations and monitor programme delivery as part of the Post-16 Planning and Funding Framework. The data is also used to support the development of consistent performance measures for post-16 learning.

School workforce annual census (SWAC)

The **SWAC** is an annual statutory data collection of information about the workforce in maintained schools in Wales. It provides comprehensive information on the school workforce which is used to inform Welsh Government policy on issues relating to the school workforce, including pay and conditions, recruitment and retention, and in calculating costs of teachers pay bill for Wales and the effect of changes upon it. The data is utilised in workforce planning, including considering; potential training requirements, subjects taught, use of supply cover, and additional roles undertaken by staff. The data is also used to monitor equality and diversity of the school workforce.

It is necessary to better understand the characteristics and the make-up of the school workforce in Wales in terms of age profile, qualifications and diversity.

The SWAC is split into two data returns: the school data return and the pay, human resource (HR) and absence data return. All maintained schools are required to submit the school data return element and all local authorities are required to return the pay, HR and absence element for school staff on their payroll. Some schools that choose to not have service level agreements (SLAs) with their local authority for HR services may also be required to submit a pay, HR and absence element of the return too.

The common transfer system

When pupils transfer from one school to another, it is important that the 'new' school has, and is able to act on, information about them. The common transfer system (CTS) provides for the secure, electronic transfer of pupil information when pupils move school. Schools (or local authorities in specific circumstances) can create an electronic file, known as a CTF (common transfer file), containing personal and assessment pupil information from the school's management information system (MIS). Files must then be sent to the pupil's next school for direct import to their MIS.

The 'system' comprises two main parts: firstly, the school MIS that holds pupil data and can generate CTFs for exchange; and secondly, a secure web based transfer site 'school to school' (s2s), where electronic data files can be safely exchanged between schools, local authorities and central administration bodies. Files are exchangeable between schools, even if they use MIS software supplied by different companies.

The statutory requirements in relation to the common transfer system

The Pupil Information (Wales) Regulations 2011 specify:

- headteachers must pass on specific pupil information in electronic format when a pupil changes school, using a CTF, within 15 days after the pupil ceases to be registered there
- if a pupil leaves a school and, after reasonable effort, a headteacher has been unable to ascertain the location of the pupil's destination school or knows the pupil is moving out of the maintained sector, they must transfer the pupil's CTF to a secure internet website provided for that purpose; in this instance, it is the lost pupil area of the s2s website

- if a headteacher from a pupil's old school receives a request from the headteacher of a pupil's new school for common transfer information or any educational record relating to that pupil, they must provide the information as soon as possible after the date on which the headteacher of the old school first learned of the pupil's registration at the new school and, in any event, no later than within 15 school days after the day on which the pupil ceases to be registered at the old school
- if a pupil arrives at a new school without their common transfer information or details of their old school, the headteacher of the new school must contact the local authority which maintains the new school to request a search of the lost pupil area of the s2s website

Problem solving

If a pupil arrives from a school in the non-maintained sector, or from outside Wales or England, a temporary or new **unique pupil number** (UPN) may need to be created for them. The new school should seek the common transfer information and educational record from the old school(s). If the pupil has previously been educated in a maintained school in England or Wales, their old UPN should be reassigned to them and the temporary UPN removed. A new UPN should only be created if the school has been unsuccessful, after reasonable efforts, in locating the original CTF.

Maintained schools should make reasonable and collaborative arrangements to obtain a pupil's educational record when they arrive from a non-maintained school. If a pupil arrives at a new school without a CTF, but the details of the old school are available, the new school needs to contact the old school and request they send the pupil's CTF.

Should a child arrive at a new school without a CTF and it is established that the CTF has been sent to another school, the sending school, not the receiving school, needs to contact the incorrect school to redirect the CTF. The sending

school must then resend the file to the receiving school.

Safeguarding

If a child arrives at a new school without a CTF and their old school is not known or has no record of them attending, the headteacher should contact the local authority that maintains the school to request a search of the lost pupil area of the s2s website. Where no records can be identified, local authorities will wish to consider whether the lack of data may be a potential indicator of a family in need or at risk. In view of the potential safeguarding issues that may lie behind such cases, local authorities are strongly encouraged to process similar requests from schools in the independent sector, where those schools have made reasonable, but unsuccessful, enquiries.

Children missing education, the lost pupil database and s2s website

Revised **statutory guidance** was published in 2017 in order to help prevent children and young people from missing education. The document sets out guidance for local authorities on arrangements that will enable them to establish the identities of children residing in their area who are not receiving a 'suitable education'.

The 'lost pupil database' is a searchable area of the s2s website containing CTFs of pupils where the destination (or next) school of the pupil is not known to the school the pupil is leaving. It enables local authorities to identify pupils whose destination on leaving a school which they maintain is unknown. It also provides a facility whereby a local authority, at the request of a school enrolling a new pupil (but cannot identify the previous school to request a CTF), can search for a CTF which may have been 'posted' there by the previous school. The site currently only allows local authorities to undertake searches for a pupil's CTF. If

a school requires a search to be undertaken they should contact their authority's named lost pupil contact.

s2s is a secure data transfer website available to schools and local authorities in Wales and England. It was designed and is managed by the UK Government Department for Education, to enable CTFs to be sent from, and to, any maintained school. A generic file transfer facility also enables s2s users to exchange files of any safe type securely by following a file name convention. For schools there is a file size limit of 4Mb. For local authorities the limit is 10Mb. Files approaching that size can cause performance to degrade significantly. If possible, please split large files into sub-files (for example two or three zip files rather than one very large composite file).

Further guidance on the lost pupil database and s2s can be found in Section 6 of the **statutory guidance**.

Pupils moving out of the maintained sector

Should a pupil leave school and is confirmed to be educated otherwise than at school, moved to a non-maintained school or to a destination incapable of receiving a CTF, the school should remove the pupil's name from the school roll and send the CTF to the lost pupil section of the s2s website.

The school will need to create a CTF for that pupil only and identify the destination school as non-maintained (using MMM as the local authority number and MMMM as the school establishment number). The CTF will then be stored in the database of pupils who have moved outside the maintained system.

Further guidance on the common transfer system and lost pupil database can be found **Educational records, school reports and the common transfer system: guidance for schools and local authorities**.