General Data Protection Regulation (GDPR) Policy

This document was: Generated by SMT/School Staff in July 2018

Latest Review/ Revision by the Standards Committee -13th March 2019; 23rd September 2020; 16th March 2022

Approved at a meeting of the full governing body on 27th March 2019 ; 21st October 2020; March 23rd 2022;

Reviewed/Revised/ Approved at a meeting of the full governing body held on 24th October 2018; 26th October 2022; 21st June 2023

Review date: June 2025

Signed: _____ Chairperson schools governing body, on behalf of the governing body.

Date: _____

Signed: _____ Headteacher

Date: _____

Distribution: Staff, governors, pupils, parents/carers and the wider community as requested.

The United Nations Convention on the Rights of the Child (UNCRC) is the most complete statement of children's rights ever produced and is the most widely-ratified international human rights treaty in history. This policy relates to Article 16 of the UNCRC.

Article 16: Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Ysgol Ty Coch Special School is a Rights Respecting School.

As a Rights Respecting School, we aim to embed children's human rights in our ethos and school culture. We base our practice on the principles of equality, dignity, respect, non-discrimination and participation. Working within these principles not only empowers our children and young people, but also leads to enhanced learning, improved standards and better relationships.

1. **General Data Protection Regulation (GDPR) Policy**

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

Ysgol Ty Coch Special School collects and uses personal information about staff, pupils, parents and other individuals who come in contact with the school. The information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure the school complies with its statutory obligations.

The school has a duty to inform individuals including parents and pupils of the information that it holds. This policy document should summarise why the data is held and any other parties to whom this information may be passed on to.

2.Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely in line with General Data Protection Regulations (GDPR). It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

3.Our Commitment:

The school is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the General Data Protection Regulations.

4.Legal Basis

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements. The legal bases for processing data are as follows:

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

5. Personal and Sensitive Data:

The school has a data map which details all data in use across the school. All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

- Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information

The principles of GDPR shall be applied to all data processed and are underpinned by 7 enforceable principles: The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

6.Roles and Responsibilities

The members of staff responsible for data protection are:

- Julia Render– Senior Data Protection Co-ordinator
- David Jenkins – Headteacher until 31.08.23 , then Simon Wilson from 01.09.23
- Lyn Bundy – Office Manager, based at Tonteg
- Andrea Herman – School Clerk, based at Buarth Y Capel
- Ashlie Holland – Online Safety Co-ordinator
- Chair of Governors – Janice Stuckey

GDPR is a collective responsibility and all staff must treat all personal/sensitive information in a confidential manner and follow the guidelines as set out in this document. The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through our training programme. The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

7.Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

8. Individuals' Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

9.Privacy Notice: (Appendix 1)

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example Welsh Government, local authorities, ESTYN, or University Health Board. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- which would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

10.Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required, these organisations shall provide evidence of the competence in the security of shared data.

11.Subject Access Requests:

All individuals whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

David Jenkins, Headteacher, until 31.08.23 and then Simon Wilson from 01.09.23

Ysgol Ty Coch

Lansdale Drive

Tonteg

CF38 1PG

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from our school to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. This will aid continuation, which should ensure that there is minimal impact on the child's academic progress as a result of the move

- **Examination authorities**
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.
- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- **Social workers and support agencies**
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.
- **Right to be Forgotten**
  Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

12.Location of information and data:

Electronic Records

The use and storage of personal/sensitive data in electronic/digital format is explained in the online safety policy. The use of data in electronic/digital form is bound by the 7 principles of the GDPR. The school's main electronic platform is SIMS. The school also uses Parentmail for its communication with parents, EVOLVE for planning Educational Visits and Google Applications for curriculum resources. All platforms are accessed by passwords which are suitably complex. All platforms should be shut down after each use.

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information, individual education plans and positive handling plans that may require immediate access during the school day.

Sensitive or personal information/data should not normally be removed from the school site. However, the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils. Reasonable precautions should be taken to safeguard the information.

If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

Staff would not ordinarily transport data away from the school as it is discouraged in the online safety policy. The use of encrypted USB sticks would be used in exceptional circumstances.

If it is necessary to transport data away from the school, it should be downloaded onto a school supplied, encrypted USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

USB sticks that staff use must be password protected and supplied by the school. These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Individuals' network areas should be regularly maintained and de-cluttered to ensure no unwanted duplication.

Paper Records

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

13.Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections.

The school also uses high quality shredders to dispose of paper assets

14.Breaches of GDPR

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This will be done within 72 hours of the school becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the school will inform those individuals without undue delay.
- The school has robust breach detection, investigation and internal reporting procedures in place.
- The school will keep a record of any personal data breaches, regardless of whether you are required to notify.

COVID 19

On March 18th, 2020 the school closed to pupils in light of the Coronavirus pandemic/regulations put in place by the Senedd. From March 23rd to June 26th 2020, the school was repurposed as a childcare Hub for children of key workers and those pupils classed as vulnerable. Since then the school has made a number of changes to its operations to ensure the safety of school users. These changes impact on all elements of the school systems, processes and procedures, including distance learning.

Ysgol Ty Coch Distance learning policy update to ICT Policy

Adapted from: Safeguarding Considerations for Distance Learning v3 3.6.20

The following document has been revised following publication of further advice by Welsh Government. The most relevant current documents are linked below.

Stay Safe. Stay Learning: supporting the education system

https://gov.wales/stay-safe-stay-learning-supporting-education-system

Live-streaming safeguarding principles and practice for education practitioners https://hwb.gov.wales/zones/online-safety/live-streaming-safeguarding-principles-and-practice-for-education-practitioners/

Developing approaches to support distance learning

https://hwb.gov.wales/distance-learning/developing-approaches-to-support-distance-learning/

Advice is changing on a frequent basis and it is recommended that schools consult the Hwb Distance Learning support pages for the most accurate and up to date information, available on the following page:

https://hwb.gov.wales/distance-learning/#what-tools-are-available?

Synchronous vs Asynchronous Communication with pupils

Asynchronous approaches provide greater flexibility and can be easier for parents/carers and learners to manage at home, so should be the main approach considered by schools and settings when organising distance learning.

However, headteachers may consider synchronous approaches to be appropriate in specific circumstances in support of learner engagement and well-being. Where this is the case, governing bodies and headteachers MUST have full regard to safeguarding and Welsh Government guidance referenced above.

Considerations

Accountability

Decision-making at a school level may determine whether live streaming is appropriate to host lessons with learners. As in any school setting, all accountability is owned by the headteacher and governing body of the school. Headteachers and governing bodies must ensure that the Welsh Government guidance referenced in this document is observed alongside local authority guidance. Any live streaming should be done on a voluntary basis and staff should not be directed to undertake live streaming of lessons.

Acceptable use

The acceptable use policy that is used for the use of technology in school should be applied when using technology for distance learning for both staff and pupils. The Hwb also provides a 360 degree Safe Cymru tool to support the school's online safety policy and practice available at the following link:

https://hwb.gov.wales/zones/online-safety/repository/resource/6f3b56cd-439c-49a9-bc64-696223b85466/en

Platforms

Direct communication with students/parents should be carried out using SeeSaw, school Google email, RCT corporate emails and other approved platforms/devises such as class Hwb, TEAMS and mobile phones.

Careful consideration should be given to the privacy notice and the level of control and security in place to safeguard all involved. School provided accounts should be used by pupils and school provided devices used by staff.

Professional Issues

Live streaming of lessons (synchronous teaching) **is only permitted with the explicit permission of the Headteacher**. Any education practitioners choosing to live stream should continue to work in the same professional manner as they would in the classroom. There should always be at least two members of teaching staff online and present at all times during any live-streamed lesson. One-to-one live-streaming lessons with learners should not be undertaken and consideration given to the fact that all comments will be heard by a number of learners and could be potentially misconstrued. Consideration should also be given to confidentiality when live streaming a lesson from a venue where other adults or children are present. The school does not permit recording of synchronous activities.

If lessons are recorded to be shared with learners at a later date, this should be done as an **asynchronous** activity without learners being present in the recording. Recordings must not be used for any teacher evaluation purposes.

Asynchronous

Asynchronous sessions give both learners and teachers flexibility and a safer environment to work in, minimising the unexpected whilst ensuring interaction. Pre-prepared video, podcasts and other content can be posted through the chosen learning platform and an outline provided to pupils as to how they can post responses.

Setting

If pupils are asked to record and submit any work via video, or take part in synchronous learning activities, clear advice should be provided about the setting. For pupils and staff it would be inappropriate for them to be in their bedroom for example. Pupils should be encouraged to be in a social space, preferably accompanied by their parent or other adult and ensure that the background is free of inappropriate/personal items. Staff must also be alert to the pupil and their own setting and the possibility of others in the background displaying inappropriate behaviour/language and pupils seeing a member of staff's personal items. Many platforms allow staff to change their background setting and this should be used where available by staff and learners.

Network connection

Consideration should be given to the fragility of each pupil's network connection (or if they even have one). Children are likely to get stressed if their internet connection cannot effectively engage with the technology being used and could potentially fear of missing out in an educational environment. Homes with multiple learners and parents working from home may also mean a lack of equipment to use. Wi-Fi use should be encouraged to avoid potential network costs if learners choose to use mobile phone data.

Length of session

Sessions should be kept as short as possible and used to give a brief overview of the topics that need to be covered in a given time period. Tasks can be set, submitted and reviewed before the next session. At the end of any synchronous sessions, care should be taken to ensure all learners have left before staff leave. This way staff will ensure that they are not facilitating an environment where learners are alone and unsupervised in an online room which has been created by them.

Behaviour

Clarity should be provided about the expectations of both student and staff behaviour (e.g., a 'classroom standard' of behaviour/appropriate clothing/language is expected from all participants).

'Live-streaming safeguarding principles and practice for education practitioners' (link above) contains **an example agreement for use in live streaming activities that could be disseminated to learners/parents prior to using this approach.**

This is something that I will look to produce an exemplar of and use with Post 16

Digitally Excluded Learners

Distance learning may not be possible for some digitally excluded learners. These need to be identified by schools and alternative models of distance learning explored. In the interest of equity, offline learning activities should be provided for all learners unable to access technology while the issue of their connectivity is being addressed

Further Information

Information Commissioners Office – www.ico.org.uk

Appendices

- Privacy Notice
- Consent Forms
- Parentmail consent forms

Appendix A

Equal Opportunities

The school operates a policy of equality for all pupils regardless of gender, ethnicity, religious beliefs or culture.
All staff at Ysgol Ty Coch Special School take account of each pupil's learning styles/needs and their development and wellbeing; and how these are affected by a range of social, religious, ethnic, gender, cultural and linguistic differences.
Pupils identified as Children Looked After (CLA), More Able and Talented (MAT) and those on the child protection register are supported in line with their particular needs to afford them equal access to the curriculum.

Safeguarding

The Safeguarding of pupils is of paramount importance. The school understands its duty to keep learners safe and adheres to the PREVENT agenda and broader safeguarding guidelines. Regular and well planned lessons are taught in e-safety.

Staff Development

Staff will have access to in-service training as and when appropriate. This is in accordance with the school's policy for staff development. Any new developments in GDPR will be disseminated by the headteacher and the GDPR team. Any new developments in E Safety will be disseminated by the ICT PLC throughout the year.

Role of the Head teacher

- To discuss future developments for GPDR with the GPDR team
- Facilitate training and guidance on GDPR
- Develop and implementing the GDPR policy

- Take a lead role in investigating any reported incidents.
- Inform LA of any breach
- Ensure budget provision for safe disposal of information
- Promote school compliance with GDPR advice#
- Keep abreast of current legislation
- Ensure budget provision for staff training

Links to Other Policies

- Safeguarding
- Management of Health and Safety at Work
- Password Management
- Physical Security
- Disciplinary Procedure for School Based staff
- CCTV
- Online Safety Policy (including Bring your own device/working from home policy and acceptable use agreements)
- Social Media Policy
- Data processing mapping exercise
- GDPR compliance baseline
- Freedom of Information

Appendix 1

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Ysgol Ty Coch Special School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Organisational control

Roles and Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation

- **Administrator / Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts.
  - Adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- **Process for creating new accounts**
  The school community is encouraged to consider if a social media account will help them in their work, eg a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

    - The aim of the account
    - The intended audience
    - How the account will be promoted
    - Who will run the account (at least two staff members should be named)
    - Will the account be open or private/closed

  Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where

bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**.
- Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.

- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, eg. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

    - **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
    - **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
    - Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
    - If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites.

- **Pupil/Students**
  - **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
  - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
  - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- **Parents/Carers**

  - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Managing your personal use of Social Media:

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Don’t use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy

Appendix 2: - Mobile Technologies and Working from Home Policy including Bring Your Own Device

A key strategic aim of Ysgol Ty Coch is to promote an effective work:life balance for our staff. We believe that by doing this, staff wellbeing is enhanced and they are generally better placed to meet the needs of pupils. Some staff express a preference to undertake work from home. This is generally discouraged in pursuit of a work life balance. Therefore, school staff should undertake most school work when on either of the two sites.

Mobile devices have the potential to make working practices more efficient to achieve a better work:life balance. However, using these devices also creates additional risk for data security. This policy is designed to give the school's position on working from home.

Paper Based Data Security

Output paper based which contains Sensitive/protected information should not be taken off site under any circumstances.

In school, output Paper based information from ICT systems must be considered in light of its sensitivity as personal or confidential in nature. RESTRICTED information should have appropriate controls in place to protect it. A risk assessment should identify the appropriate level of protection for the information being stored. Sensitive information on printed paper on desks or in an open office must be protected by the controls for the building and other appropriate measures that could include:

- Filing cabinets or desk drawers that are locked with the keys stored away from the source
- Locked safes
- Stored in a Secure Area protected by access controls

Mobile Technologies

There are a range of mobile devices in operation across the school. These include:

- Encrypted laptop computers
- Ipads and Ipods
- Google Suite
- Encrypted Memory sticks (only if considered absolute necessity)

Personal/sensitive information should only be stored on school owned, encrypted devices. In addition, personal/sensitive information should only be stored on a school owned device if absolutely necessary to do so and should be time limited. Personal/sensitive information should only be stored in the long term on the school's servers. Personal/sensitive information should not be stored on any personal device.

Google Suite and BYOD

The school uses the Google education suite extensively across the school. Applications include:

- Google Drive
- Google Mail
- Google Classrooms

These have great potential to encourage collaborative working practices. However, they create risk. The following guidance must be adhered to when using Google Applications:

1. Google applications must not be accessed from a personal desktop/laptop computer
2. If accessing Google applications off site from a school owned device, the internet source must be secure
3. Accessing Google suites on personal devices is permitted but limited to 1 personal mobile device (ipod, ipad, android device). The device must be encrypted with 6 digit password protection or finger print recognition

Appendix 3 Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems, data and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, Google Apps, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will regularly maintain my network drives to ensure they are de-cluttered and contain no unwanted, duplicated data

I will be professional in my communications and actions when using school ICT systems:

- I will only store data on school supplied ***encrypted*** hardware (including laptops, memory sticks, personal hard drives smart phones etc). this should be limited to the shortest time possible. Long term storage of data should be limited to the school server. I will not store data on a personal device
- When using Gmail and associated Google apps, I will ensure that I only access files on a secure device supplied by the school and I will password protect the drive. I will ensure that I log out after each session and not leave the computer unattended
- I understand that the school permits access to Google suite from 1 personal device which should be encrypted by 6 digit password or finger print recognition. I understand that personal/sensitive information should not be stored on a personal device/computer
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress

to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that if I lose personal data of any kind, it will be reported to my line manager without delay
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

General Data Protection Regulation (GDPR)

I understand that GDPR relates to data which is not solely electronic in nature. I confirm that I have read and understand my responsibilities in relation to GDPR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Safeguard Paper records which should be stored in locked cupboards
- Reduce the amount of time paper records are taken off site. Where this is unavoidable, suitable controls should be in place e.g. locked suitcases, not left in cars etc.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- School data must not be stored on personal devices
- The data must be encrypted and password protected
- The device must be password protected and supplied by school
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Photographic / Media Consent Form

Ysgol Ty Coch Special School may at times use photographs, audio, and/or video recordings of students for purposes of education and publicity on behalf of the school, via the school's website, Twitter Account, Youtube and print publications. Similarly, the school may wish to share good news stories and associated pictures or video of pupils with media. These occasions arise at various points in the academic year.

In line with The General Data Protection Regulation **the school** is seeking consent from parents/carers of pupils for them to be photographed or recorded, or have their name used in connection with any such recording.

The school's Twitter feed is a closed group visible only to accepted users. Pupils photographs will never be accompanied by their names.

Completed consent forms will be recorded by the school with consent lasting for the duration of the child's time in school.

Your co-operation in this important matter is very much appreciated.

PHOTOGRAPHIC / MEDIA CONSENT FORM

Name of student ……

Consent is sought for the following, please tick all boxes that you wish to provide consent for:

I permit **Ysgol Ty Coch Special School** to produce and store imagery/video of the named individual during the course of the child's time in school, and that all copyright of the imagery/video shall remain with the school – This includes the use of the SeeSaw software	
I grant **Ysgol Ty Coch Special School** permission to use the imagery/video for future promotional purposes on the schools website, Twitter Feed and print publications ***(delete or add to as appropriate)***.	
I grant **Ysgol Ty Coch Special School** permission to use imagery/video for our channel on YouTube	
I grant **Ysgol Ty Coch Special School** permission to share the imagery/video with local and/or national media.	

Name of Parent/Carer (Print).....

Signed …… Dated ……..

Appendix 4 - Ysgol Ty Coch Special School E-Safety Parent / Carer Code of Conduct

Code of Conduct

At Ysgol Ty Coch Special School we value the strong relationship with parents and carers. Together, this helps us achieve the very best for the children in a mutually supportive partnership between parents, class teachers and the school community.

As a partnership, parents understand the importance of a good working relationship with the school. We continually welcome and encourage parent and carers to participate in the life of the school. Parents and carers are always encouraged to contact the school with any concerns and/or issues. The school would appreciate the opportunity to resolve any matter with parents and carers.

Parents, carers and visitors are reminded:

- To respect the caring ethos and values of the school;
- That both teachers and parents need to work together for the benefit of their children;
- Approaching school staff for help to resolve an issue is done in an appropriate manner; and
- All members of the school community are treated with respect using appropriate language and behaviour.

The school will not tolerate:

- Disruptive behaviour which interferes or threatens to interfere with any of the schools operation or activities anywhere on the school premises;
- Any inappropriate behaviour on the school premises;
- Use of loud or offensive language or displaying temper;
- Threatening, in any way, a member of staff, visitor, fellow parent/carer or pupil;
- Damaging or destroying school property;
- Sending abusive or threatening e-mails or text/voicemail/phone messages or other written communications to anyone within the school community;
- Defamatory, offensive or derogatory comment regarding the school or any of the pupils/parents/staff at the school on Facebook or other social sites (see appendix 1)

Should any of the above occur on school premises, the school may feel it necessary to take action by contacting the appropriate authorities and / or consider banning the offender from entering the school premises.

Appendix 1

'Social media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by providing information, signposting to services, sharing opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation, engagement, pass information and services over a wide network of people. This could include blogs, message boards, social networking websites (such as Facebook, Twitter, LinkedIn, My Space) and content sharing websites (such as Flickr, Youtube) and many other similar online channels.

Definitions of misuse or inappropriate behaviour

The following actions may constitute misuse of social media or inappropriate behaviour; it is however by no means exhaustive:

- Publishing materials that might be considered inappropriate, offensive or libellous
- Publishing materials considered to be defamatory or to the detriment of the School and its community

In the event that any pupil/parent/carer of the school is found to be posting libellous or defamatory comments on Facebook or other social media network sites, they will be reported to the appropriate "report abuse" section of the network site. The school will also expect the pupil/parent/carer to remove such comments immediately. The school will consider its legal options to deal with any such misuse or inappropriate behaviour.

Appendix 5 - Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

- I will only use ICT in school for school purposes
- I will only open e-mail attachments from people I know, or who my teachers has approved
- I will not tell other people my ICT Passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is reasonable, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidently find anything like this, I will tell my teacher
- I will not give out my own details such as my name, phone number of home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my e-safety
- If I am unsure about anything, I will ask a member of Ysgol Ty Coch staff for help

Signed (child):……

Signed (parent): ……..

Appendix 6 - Schools Data Incident Management

Summary Actions

1. **Identify a lead member of staff to manage the incident**
    a. This is likely to be a senior leader other than the deputy Headteacher or Headteacher who can act impartially, independently and without time constraints and limits.
    b. The person needs to be trusted by all members of staff where openness is key to the containment and recovery of the loss.
    c. This person will need the authority to request information from staff and to access systems that may form part of the investigation.
    d. This person will need to document all of their actions. A timeline of actions and findings will prove useful if an external investigation is undertaken by the LA or ICO.

2. **During School Hours – Contact The Local Authority**
    a. If in doubt - ring for advice. Not all breaches will deal with information that is reportable.

3. **Establish the nature of the incident e.g.**
    a. Loss or theft of equipment, paper assets or other media on which identifiable information is stored.
    b. Inappropriate access or inappropriate access controls deployed to an information system, or filing storage area.(e.g. someone has accessed files from a room such as a head of department, assistant head – access provided to an electronic file where access rights have not been secured appropriately.)
    c. Information System Failure (e.g. hardware failure)
    d. Human Error – sending information to the wrong party via post / email / fax.
    e. Environmental damage such as fire / water damage affecting equipment or paper.
    f. Hacking of network – including phishing, email malware and other intrusions.
    g. “Blagging” and other techniques to illicit information from staff members via phone or in person.
    h. Establish the amount and type of information lost, e.g. special category and the number of data subjects affected – this will help determine the response to the ICO and to the affected data subjects.

4. **Containment and recovery:**
    a. If the loss has occurred as part of a crime, or there may be a criminal component, contact the police.
    b. If the incident involved a device, establish whether it was encrypted or not.
    c. If material has been lost outside of the school, establish whether it can be recovered and take immediate steps to achieve that.
    d. If the incident involved compromising your network, engage with your ICT support and suppliers to ensure all steps are taken to remove the vulnerabilities.

5. **Assessing The Risks To Data Subjects**
    a. Based upon the information gathered in 3(h), assess the possible impact on the data subjects involved and how to mitigate against these risks.
    b. Based upon the potential risk, consider whether and how you will contact data subjects, and the level of support you may need to provide to them.
    c. Based upon the potential risk to data subjects, decide whether the incident has to be disclosed to the ICO.

6. **Evaluation and response** (Depending on the nature of the event, the ICO may decide to investigate further)
    a. Make sure you have supporting documentation relating to policies and procedures that support the safe and effective use of information and data.
    b. Ensure that the timeline recording by the coordinating officer is complete and describes all the schools actions.
    c. Once the incident is under control, undertake a full impartial investigation into the reasons for the loss, and implement mandatory procedures to prevent a reoccurrence.

Appendix 7a – Ysgol Ty Coch Special School

Privacy Notice

(Parents, Guardians, Pupils)

How We Use Parent, Guardian, Staff and Pupil Information

The categories of pupil information that we collect, hold and share include:

- ✔ Personal information (such as name, unique pupil number and address)
- ✔ Special Category (such as ethnicity, health, language, nationality, country of birth, sexual orientation and free school meal eligibility)
- ✔ Biometric Information such as finger print recognition for school meals
- ✔ Attendance information (such as sessions attended, number of absences and absence reasons)
- ✔ Assessment information (such as results of Welsh national test, statutory assessments in years 2 and 6 and on-going teacher assessment)
- ✔ Relevant medical information given to us by parents and other third parties such as NHS Trusts, GPs and allied medical professionals (such as physiotherapists, sight and hearing impaired professionals)
- ✔ Special Educational Needs and Disability information
- ✔ Behaviour and exclusions – both internal and external

Why we collect and use this information

We use the pupil data:

- ➢ to support pupil learning
- ➢ to monitor and report on pupil progress
- ➢ to provide appropriate pastoral care
- ➢ to assess the quality of our services
- ➢ to comply with the law regarding data sharing
- ➢ to safeguard pupils

The categories of parent information that we collect, hold and share include:

- ✔ Personal information (such as name and address)
- ✔ Contact Details including telephone numbers, place of work and email addresses
- ✔ Contact details of relatives that may include names, addresses, telephone numbers and relationship with child

- ✔ Legal access to the child and any court orders indicating access rights
- ✔ Social Service involvement with families.
- ✔ Information relating to whether a parent is a member of the armed forces.

Why we collect and use this information

We use the parent data:

- To be able to contact you in relation to the pupil's educational provision, and also in the case of urgency.
- In order to engage services from other organisations, such as the Local Authority.

The lawful basis on which we use this information

On the 25th May 2018 the Data Protection Act 1998 was replaced by the General Data Protection Regulation (GDPR). The condition for processing under the GDPR will be:

Processing pupil, parental and carer information is necessary for the school to undertake its statutory responsibilities. This is called in the 'Public Interest' and is where the school is exercising official authority which is laid down by law.

Where the school does not have a statutory basis for collecting and processing the data, e.g. information for a school trip, the school will request your explicit consent to gather and process the information and you will always have the opportunity to opt out of this process. However, in these circumstances, opting out will often prevent the activity taking place.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data in line with the guidance set out in the **Retention Schedule contained within the IRMS Toolkit for Schools**.

- The education record of all pupils will be processed and retained until the pupil leaves the school.
- For the purposes of inspection by ESTYN, some records are retained.
- On some occasions, the school has a legal responsibility to retain information for future access. Eg safeguarding and wellbeing.

Following the retention period expiry, information will be destroyed securely and permanently.

Who we share pupil information with

We share pupil information with:

- The Welsh Government *
- Supporting Local Authority *
- Other Local Authorities *
- The Central South Consortia *
- Schools that the pupils attend
- Safeguarding Boards
- Examination Boards where appropriate *
- Companies that undertake analysis of performance data
- Children and Family Wellbeing Services
- Hospital Trusts
- IT Services such as the Welsh HWB Learning platform (requires consent)
- School to Parent Communication Services
- Employment and career advice organisations
- Police or other law enforcement agencies
- Health and Safety Executive
- Private sector and voluntary organisations where they provide services for the school.

For Privacy Notice information relating to the identified * organisations, we refer you to their websites

Why we share pupil information

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

We share pupils' data with the Welsh Government and the Local Authority through the Central South Consortium on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Welsh Government under the Education Wales Act 2014 and associated regulations for testing, assessment and other statutory duties.

Vital Interest Information

In circumstances of the wellbeing and safeguarding of the child, it may be necessary to share information without your consent or knowledge.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please make your request in writing to the school, including your contact details and we will contact you.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations
- If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

The General Data Protection Regulation (GDPR) gives you important rights:-

1. The right to be informed
2. How you can access your information
3. Ensuring your information is accurate
4. Making sure your information is deleted in an appropriate timeframe
5. Ensuring that your information is only used for the purposes for which it was gathered
6. Ensuring that your information is transferred in an agreed and secure format when your child move educational establishment
7. In certain circumstances the right to object

Rights in relation to automated decision making and profiling

The school uses a wide range of data regarding pupils in order to provide support and guidance pertinent to their needs. This process is not solely automated and the parent will always have the opportunity to provide additional information. E.g. during open evenings or IEP reviews

Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer.

Approved by: The Governing Body Date: 26th October 2022

Next review due by: Autumn Term 2024

Appendix 7b – Privacy Notice (Staff)

Ysgol Ty Coch Special School

School Workforce Privacy Notice

How we use your personal information

For Workforce Administration

Who we are and what we do

Ysgol Ty Coch Special School is an employer and provides educational services for the local community. Undertaking this work means that we must collect, use information and keep records about our workforce. This includes employees and workers such as teachers, lunchtime supervisory assistants, learning support assistants and caretakers.

Ysgol Ty Coch Special School is an educational provider and is managed by the Governing Body. It is supported to deliver its functions via a formal relationship with the Local Authority – Rhondda Cynon Taf County Borough Council.

Data from employees and workers are used to manage the employment contract, which includes monitoring performance and attendance, training and development and payroll. These functions are delivered by the Local Authority (LA), and includes services such as Payroll and Pensions, Human Resources, Occupational Health Services and Training.

We collect and use personal information about our workforce and we must therefore make sure that you know what we intend to do with your information and with whom it may be shared.

The School's workforce is its most valuable asset and resourcing, developing and maintaining good employment conditions and practices for all staff is important so we also use summary data to ensure effective planning.

We have summarised in this privacy notice some of the key ways in which we use your personal information for workforce administration purposes. If you are a volunteer, some parts of this privacy notice will not apply to you, for example processing of data for payroll purposes.

Whose personal information do we collect and process?

The types of information that will be processed typically includes:

- Personal details e.g. name, address, date of birth
- Contact details e.g. email address and telephone number

- National Insurance Number
- Gender
- The terms and conditions of your employment
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and within the School
- Information about your remuneration, including entitlement to benefits such as pensions
- Pay information to include gross (before deductions) and net (after deductions) figures
- Historical pay and hours information, used for Pension purposes (in order to resolve queries from the Pensions Section who calculate your pension benefits for support staff and Teachers' Pensions for teachers)
- Deduction from pay and 'payments over' of Council Tax, Prudential Additional Voluntary Contributions (AVC's) and various membership fees, i.e. Trade Unions, Welsh Hospitals and various charity organisations (under Give as you earn arrangements), if paying through your salary
- Details of any attachment or earnings (Court orders) you may have
- Salary sacrifice deductions from pay and submission of the P11D to HMRC at year end to report on any taxable benefits where eligible in accordance with your terms and conditions of employment
- Your bank or building society account details
- Information about your marital status, next of kin, dependents and emergency contacts
- Information about your nationality and entitlement to work in the UK
- Information about your criminal record, if it is essential to your job role
- Details of your schedule (days of work and working hours) and attendance at work
- Details of periods of leave taken by you, including holiday, sickness absence, family leave, and the reasons for some types of leave
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence, which are held in accordance with the relevant Human Resources Policies
- Assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence
- Information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments, if you have declared this information
- Equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief, if you have declared this information

Where does the school get its information?

The school may collect this information in a variety of ways:

- Through application forms, CVs

- From your passport or other identity documents such as your driving licence, which are collated during your pre-employment suitability checks
- From correspondence with you.
- Through interviews, meetings or other assessments, for example supervisions, performance reviews and appraisals and return to work interviews.

In some cases, the School may collect personal data about you from third parties.

These may be things such as references supplied by former employers or tutors, information from a Regulator or court case outside of work and social media, information from employment background checks, providers which include but are not limited to regulatory bodies, information from credit reference agencies and information from criminal records checks permitted by law.

The school also generates its own information about its staff, for example during staff performance reviews, or with the Local Authority when undertaking work such as grievance or disciplinary processes.

What does the School do with your personal information?

Processing your data allows the school to:

- Run safe recruitment and promotion processes
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee and worker contractual and statutory rights
- To pay your salary and any additional payments you may be owed each month
- To pay your Employment taxes over to HMRC
- Be satisfied as far as we can be of your suitability to be employed in the role you are contracted to work
- Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace which are held in accordance with the relevant Human Resources Policies
- Operate and keep a record of employee and worker performance and related processes, for example training and development, plans for career development, and for succession planning and workforce management purposes
- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees and workers are receiving the pay or other benefits to which they are entitled
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that the employee and worker are receiving the pay or other benefits to which they are entitled
- Ensure effective general Human Resources and business administration
- Provide references on request for current or former employees and workers
- Respond to and defend against legal claims

- To provide the Pensions Section or Teachers' Pensions with pay and hours information for the production of an annual Benefits Statement
- For statistical and financial modelling.

Processing special categories of personal data

Information about ethnic origin, sexual orientation or religion or belief are processed for the purposes of equal opportunities monitoring. This is to carry out its obligations and exercise specific rights in relation to employment. Data that the school uses for these purposes is anonymised and employees and workers choose whether to disclose this information. They can also request that the organisation does not process this data for equal opportunities monitoring at any time.

Employees and workers are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

What is the legal basis for the school to use this information?

We use your information to process data to enter into an employment contract with you and to meet obligations under your employment contract. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefits such as your pension.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations, e.g. to check an employee's or worker's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees or workers to take periods of leave to which they are entitled.

Your information may also be processed to carry out a task in the public interest or in the exercise of official authority in our capacity as a public body, for example by providing volunteering opportunities and by listing staff contacts within the school.

Does The School share my personal information with any other organisation?

For the School to undertake its duties in relation to the employee and worker administration function, we may be required to provide information to the following:

In the event of any disputes or grievances we will share the relevant information with employee appeals panels, the school's governing body and the relevant local authority services.

Dependent upon the type of your contract we will also share your information with other organisations and relevant professional regulatory bodies such as:

- Accreditation bodies for individual qualifications and service standards.
- Department For Work And Pensions (DWP)
- Teachers' Pensions
- Welsh Government
- Education Workforce Council
- HMRC
- Disclosure and Barring Service
- The Police

- Local Safeguarding Children Board
- Other Local Authorities
- Credit Reference Agencies
- Training Providers / Developers
- Recruitment Consultants and Companies such as Eteach.
- Solicitors
- Independent Registered Medical Practitioner (IRMP) if required for pension administration
- Prudential
- Welsh Hospitals
- Former employers
- Prospective employers
- Trade union representatives
- Legal advisers, for the purpose of receiving employment law advice

How long will my information be kept?

We will only keep your personal information for as long as we need it. In practice, this means that your personal information may be retained for a period of between 6 months and as for long as you are employed by the School. We also keep some of your information if your employment ends, this is necessary to comply with government regulations in respect of records management, and also to enable the Council to provide information for such things as references and pension administration.

Your information, your rights

The General Data Protection Regulation (GDPR) gives you important rights, including the right to access the personal information the services hold about you.

Contact us

If you have any concerns or would like to know more about how the school uses your personal information please contact us in one of the following ways:

- By letter addressed to Mr David Jenkins– Ysgol Ty Coch, Lansdale Drive, Tonteg CF38 1PG
- By email to: Admin.ysgoltycoch@rctcbc.gov.uk
- By telephone 01443 203471
- In person to your line manager within the school.

COVID-19 Track and Trace Privacy agreement How we use your personal information for COVID-19 Contact Tracing purposes when you attend/visit our School

In the course of a school day we must collect and use information about pupils, parent/carers, staff and visitors. Because we collect and use personal information about individuals we must make sure that they know what we intend to do with their information and who it may be shared with.

We have summarised in this privacy notice some of the key ways in which we use your personal information for Contact Tracing purposes when you attend/visit our School.

This information should be read in conjunction with the School's Privacy Notice

1. Who we are, what we do.

You will be aware from the media and in particular from Welsh Government and Public Health Wales, of the Test Trace Protect scheme, which is key in the on-going fight against COVID-19 (Corona virus) and helping to find a way for people in Wales to live and work alongside the virus whilst containing its spread.

Contact tracing is a known method of controlling the spread of an infectious disease, it is not about surveillance or enforcement but about protecting people's health.

As lockdown restrictions are eased and Schools reopen, there is a requirement for the School to keep a register of people who attended its premises for Contact Tracing purposes.

Access to our School may be refused, for the safety of our pupils, staff and visitors, if you refuse to provide us with your details.

2. What and whose personal information we hold?

We will keep a record of any person who attends or visits our School, using both the pupil attendance register and visitor logs. This may include but is not limited to:

- Pupils
- Staff member
- Parents/carers
- Volunteer
- Member of the public
- Visitor
- Governor
- Elected Member

We will keep a record of the following information;

- Your name
- Contact details – email/telephone number
- Date and time of your visit or attendance at School.

3. Where does School get my information from?

Pupil's information will be taken from the attendance register and contact details (telephone number and/or email address) from school's records. In the case of primary age pupils, parent/carer contact information will also be provided from school records.

Staff data will be taken from SIMS.

All other visitor's, including parents and carers information will be taken from the visitor's signing in book/system.

4. What will we do with your personal information?

If the Local Authority is made aware of a positive Coronavirus case within a school, they will inform the Contact Tracing Team, who then work with the relevant departments within the Local Authority and Schools to ensure the necessary contacts are undertaken.

If someone tests positive for Coronavirus and informs the Contact Tracing Team that they have recently attended our School, the Contact Tracing Team will contact the Headteacher to request the information of all attendees for the relevant period.

Note that in the case of primary age pupils, their parent's contact information will also be provided to the Contact Tracing Team.

5. What is the legal basis for the use of this information?

The legal basis for processing your personal data for contract tracing purposes under the General Data Protection Regulation (GDPR) is:

- Article 6(1)(e) – Task carried out in the public interest or in the exercise of official authority vested in the controller

This is supported by the following legislation:

- Regulation 12 of the Health Protection (Coronavirus Restrictions) (No. 2) (Wales) Regulations 2020.

6. Does the School share my personal information with any other organisation?

As explained above, if required the School will share your information with the relevant Contact Tracing Team.

Contact Tracing Teams operate across the whole of Wales and are jointly delivered by Local Authorities, Health Boards, NHS Wales and Public Health Wales.

Your information may be shared with Contact Tracing Teams from any of these organisations, depending on the area in which the confirmed case originated and the organisation leading the case.

Your information may also be shared with such organisations in England, Scotland etc. (for example in the case of cross border travel).

7. How long will my information be kept?

The School will keep your information, for the above purposes for 21 days from the date of your visit.

Please note pupil attendance registers and visitor logs will be keep for a longer period of time for other purposes.

8. Your information, your rights

The GDPR gives you important rights. To find out more about accessing personal data and the other rights, please visit our School's general privacy notice.

9. Contact us

If you have any concerns or would like to know more about how your personal information is being used for Contact Tracing purposes, please contact us at:

YSGOL TY COCH
Lansdale Drive
Tonteg
Pontypridd
CF38 1PG

head@ysgoltycoch.co.uk

Appendix 8 - Appropriate Transfer of Personal Information

Contents

Appropriate transfer of personal information

Personal and commercially sensitive information can be found in many different formats within the workplace, from electronic information stored on computer, laptops, tablets and mobile phones, to paper information stored in files, folders, handwritten diaries and notebooks etc.

This guidance aims to highlight the potential risks associated with each of these transfer methods and raise awareness of the measures to support the mitigation of those risks. This will enable you to make better informed choices based on the sensitivity and the urgency of the information being transferred.

1. What is personal information?

Personal information means information, which relates to a living individual (the data subject) and from which that individual can be identified. This can include factual information such as name, address, date of birth etc or descriptions, opinions. It can be in paper, electronic (computer), photographic, audio or other format.

2. Why do we need to safeguard personal information?

The GDPR states that organisations must have appropriate technical and organisational measures in place to prevent unauthorised or unlawful access to personal information and to prevent accidental loss, destruction or damage to personal information.

3. What are the consequences if we fail to safeguard personal information?

If we fail to safeguard information it can affect all those involved:

Data Subject (the individual whose personal information we've failed to safeguard) - if personal information is lost or is accessed by someone who isn't entitled to see it, then the data subject could potentially be at personal risk, suffer damage to their reputation, fraud or identity theft.

Staff Member - The School has a number of Information Management policies and procedures in place which govern how we manage information and this helps us to comply with the requirements of the GDPR. If these policies are breached, it may be necessary to undertake a formal investigation.

The Organisation - The Information Commissioners Office, who oversees the GDPR, can take action against an organisation for breaching the GDPR. Dependent upon the nature and impact of any information breach, the ICO may issue advisory notices, undertake onsite visits to initiate further investigation and in very serious cases this may include issuing a monetary penalty notice of up to €10m.

4. Deciding on the most appropriate transfer method.

Deciding on the most appropriate way to transfer personal information and the level of security required must be done on an individual basis. You must always take into consideration:

- The **sensitivity** of the information
- The **urgency** of the situation and the tools available to you
- The **potential risks** associated with each transfer method

a. Special Category Information

Always consider the **Category** of the information you're sending and ask yourself the following questions:

- Does it contain personal information?
- Does it contain personal special category information (e.g. racial or ethnic origin, political opinions, religious beliefs, trade union membership, medical details, sexual orientation, and criminal offences -alleged or convicted)?
- How many individuals does the information relate to?
- What would the impact be if this information was inadvertently shared with the wrong people, lost or stolen? What would the impact be on the data subject?
- Think about the impact it would have on you as the person sharing the information as well as the School?

Remember! The higher the numbers of individuals involved and the more sensitive the information - the greater the impact it could have on those involved.

b. Urgency of the situation

Often the transfer method is determined by how quickly the recipient needs to receive the information. It may also be determined by what tools are available e.g. email, secure email, internet etc.

Potential risks should always be considered on an individual basis without exception.
If in doubt always seek advice from a senior member of staff in the school.

c. Potential Risks v Transfer Method

Some transfer methods carry more risks than others and should be subject to very careful
consideration. Section 6 below provides you with further guidance regarding this.

5. What happens if things go wrong?

If you encounter a problem when transferring personal information, you must notify a senior member of the school staff immediately

Things to understand when this occurs are:

- Where information has been shared inadvertently
- Where personal information has been sent to copied to the wrong person
- Where personal information has been shared excessively i.e. too much information has been shared (over and above what's required).
- Additional information has been shared outside limits of authorisation.
- Information has been shared with too many individuals
- Where personal information has been lost, stolen or hasn't arrived at its intended destination.

Further information on how to report a security breach will be addressed in bulletin 2.

6. How to transfer personal information appropriately

a. Discussion On The Telephone

What are the risks?

- Caller may not be who they say they are
- Caller may not be entitled to the information
- Others may over-hear the call – be particularly vigilant where visitors, contractors or other family members are in listening distance.

How do you reduce the risks of things going wrong?

- You must verify the caller's details - are they who they say they are?
- If the caller is a customer or client and is not known to you, verify their personal details - name, address, DOB, relevant reference number etc.
- If the caller is acting on behalf of a customer or client, check there's consent to share the information before disclosing.
- If the caller is from another organisation and is not known to you, take their switchboard number and ring them back. If in any doubt, confirm the identity with the organisation.

- Ensure that your conversation can't be overheard.
- Provide the information only to the person who has requested it and is entitled to receive it - never leave the information as a message with colleagues, another person or on an answer phone.

b. Delivering Information In Person

What are the risks?

- Information could be lost in transit.
- Information could be stolen in transit.

How do you reduce the risks of things going wrong?

- Transfer information electronically on an encrypted device wherever possible.
- Only leave the information with the intended recipient.
- Paper information must be transported in a sealed file/envelope.
- Perform double checks to ensure that correct information is being sent.
- When delivering, information must not be left unattended.
- When transporting by car ensure the information is placed in the boot and locked.
- If transporting on foot ensure the information is stored out of sight in a bag etc.

c. Postal or Courier Service

What are the risks?

- Potentially higher risk if sending hard copy paper information. Risk can be reduced if using an electronic copy on an encrypted portable device.
- Information could be lost in transit.
- Information could be stolen in transit
- Information could be delivered to wrong address/recipient.
- Receipt of information can't be guaranteed.

How do you reduce the risks of things going wrong?

- Encrypted portable devices must be used wherever possible & password provided separately - email/telephone call etc.
- Mark the envelope for the attention of a named individual not just the company or department name.
- Ensure the address is correct and clearly stated - always include a postcode.
- Seal the information in a double envelope.
- Double check that correct information is being sent.
- Ensure a return address and contact name is marked on both the outer and inner envelope in case of non-delivery.
- Ensure the envelope is fit for purpose and can withstand transit - use tamper proof envelopes where required.
- Use recorded or special delivery where appropriate so that the parcel can be tracked.
- Request confirmation of receipt.

d. Web Upload / Database Access

What are the risks?

- Could be intercepted if no secure connection.
- Site could be accessed by individuals who are not entitled to see the information.
- Must rely on recipient to verify that site is secure.

How do you reduce the risks of things going wrong?

- Use approved Local Authority and Public Sector transfer portals where available.

e. Email

What are the risks?

- The email could be sent to the wrong email address
- Emails sent outside of the School **(that are not encrypted)** are considered generally "unsecure" as emails are transferred via the public accessed internet and could potentially be intercepted.

How do you reduce the risks of things going wrong?

- Only send emails containing personal or special category information using official school based email addresses such as @rctcbc.gov.uk
- Only send to other schools or local authority formal email addresses e.g.@merthyr.gov.uk / @bridgend.gov.uk or Consortia email addresses e.g. @cscjes.org.uk
- Ensure that the email is addressed to the correct recipient
- Ensure that the correct information is being sent
- Double check you have the correct email address or if selecting from a user list or directory that the correct person is actually selected **(be aware of users with the same/similar names).**
- Do not send personal or sensitive information to a distribution list, unless you are absolutely sure that the members are up-to-date. Remember Distribution Lists are managed by you not central systems.
- Beware of auto-populate when selecting the recipient's name i.e. an email address maybe suggested to you upon typing the first few characters of a name. Ensure it's the correct address.
- Clearly mark the subject heading of your email 'confidential'.
- When sending to external email addresses, personal information must be sent via an attachment and must not feature in the body of the email text. The attachment must be password protected.
- Send the password to the recipient separately i.e. in a second email for additional security (a 2 email rule).
- Double check that the correct information is being sent.
- Request a delivery and read receipt.

- Staff use of email for school based communication should be restricted to @hwbmail.net / Google classroom email addresses or local authority provided email addresses such as name@rctcbc.gov.uk

- Schools with their own email servers need to identify through their IT support that their email systems are GDPR compliant.

g. Fax

This method should only be used if no other more secure method is available and then used with extreme caution.

Staff Responsibilities

- ✔ Familiarise yourself with the transfer arrangements for your site - there may be internal procedures which dictate how information is transferred i.e. via post, secure email etc.
- ✔ Ensure that you select the correct method of transfer in relation to the sensitivity and format of the information being transferred.
- ✔ Ensure that you familiarise yourself with the Procedure for Reporting Information Security incidents and events.

Managers responsibilities

- ✔ Ensure that staff are made aware of the transfer arrangements for your site - you may have internal procedures which dictate how information is transferred i.e. via post, secure email etc.
- ✔ Ensure that staff select the correct method of transfer in relation to the sensitivity and format of the information being transferred.
- ✔ Ensure that e information is stored securely whilst awaiting disposal.
- ✔ Ensure that staff familiarise themselves with the Procedure for Reporting Information Security incidents and events.
- ✔ Ensure that you familiarise yourself with the Procedures for Reporting and Investigating Information Security incidents and events.

Appendix 9 - Protecting Personal Information

Outside School

Contents

Protecting personal information outside of the school environment

When travelling and working with personal information outside of the school environment, information becomes more vulnerable and susceptible to loss, theft and compromise. Extra care must be taken to protect the confidentiality of personal information and measures taken to avoid unnecessary risks to that information and the people it is about.

This guide provides staff with good practice guidance on protecting personal information when transporting and using outside of the school environment.

1. Why do we need to protect personal information?

GDPR requires organisations to have appropriate measures in place to protect personal information that we are responsible for from being lost, mislaid or stolen, and the information potentially being accessed by people who aren't entitled to see it.

GDPR states that any measures taken should be appropriate to the sensitivity of the information, and the potential damage and distress, theft or loss could have on the individuals who are the subject of the information.

2. What happens if we fail to protect personal information?

If we fail to protect personal information properly it can affect all those involved:

The individual - If personal information is mislaid, lost or stolen or is accessed by someone who isn't entitled to see it, then the individual could potentially be at personal risk. They could potentially suffer distress as a result of damage to their reputation, fraud or identity theft etc. Loss of information may also affect the services a person receives, or may require the information to be collected again.

Staff Member - If a member of staff loses or mislays information then the matter will need to be investigated by a senior manager.

The Organisation - The Information Commissioners Office (ICO), who oversees and enforces the GDPR, can take action against a school if they have failed to look after personal information properly and have broken the law. In serious cases the ICO can issue fines of up to €10M for serious breaches of the regulations. A school could also suffer reputational damage as a result of bad publicity and incur additional costs to put things right.

3. Things to consider before taking personal information outside school.

Before taking personal information outside of school, you must consider the sensitivity of the information being removed, the format in which the information will be held and where it is being taken. By planning ahead you will be able to identify any potential risks and plan better to safeguard against them.

This does not mean that staff cannot work at home. This is about the appropriate safeguards being in place to ensure that personal or special category data is handled securely.

Theft and loss of information should always be your primary concern, but information can also be overlooked, overheard or left behind, so these issues also need to be considered.

Before you remove any personal information from school, ask yourself the following questions:

a. How much information is it necessary to take with you?

You should always ask yourself whether you really need to take the information outside school.

You should consider whether there are other alternatives to removing personal information from the school - for example,

- Is it possible to take a summary of the information, excluding or limiting personal identifiers such as name, address, date of birth etc, as opposed to the full data set?
- Do you need to take all of the information e.g. the entire file, or only essential, relevant information contained within it?
- Could the information be accessed securely by electronic means? (see 4a)

You should never carry personal information around on the off-chance you might need it, or look at it if you have the time - this is just creating extra risk for no real purpose.

Paper copies of original information should have a footer such as:

This information is a copy of a protected document and may be of a personal nature of special category. Once the document has been used it should be destroyed securely.

The date the information is printed should be included in the footer as well as the page identifier i.e. Page 1/4

b. What information am I taking?

Consider what information is being taken outside of the school - is it personal, special category Consider how many individuals the information relates to? Remember - the more sensitive the information and the higher numbers of individuals involved, the greater the potential impact if lost, mislaid or stolen.

Think about the potential impact if the information is mislaid, lost or stolen? What would the impact be on the individual who is the source of the information (identify theft, fraud, physical harm), you as the person responsible for losing or misplacing the information (potential investigation at work), and the Council (bad publicity, potential fine of up to £500k from the Information Commissioners Office)?

c. What format is the information in?

Different formats of information storage present difference risks - unlike electronic encrypted devices (eg laptop, USB memory stick), personal information in paper format cannot be protected if lost, mislaid or stolen and is therefore potentially accessible by anyone who comes across it.

The most secure and appropriate method of transporting personal information must always be used i.e. electronic encrypted media devices. Further information on this can be found in section 4a of this guide.

4. Protecting personal information outside school.

a. Information Format

Wherever possible personal information must be transported using a **school approved electronic encrypted device** such as a laptop, tablet or USB memory stick.

Personal devices must never be used as they may not be fit for purpose and have the latest encryption and antivirus technologies installed. In addition, personal devices are often shared and used by family members or friends, who could potentially access personal information that they aren't entitled to see.

Personal information in paper format must not be taken outside the school **unless it is absolutely necessary** and all other, more secure options such as electronic encrypted devices are not available.

If personal information in paper format is permitted to be removed from school you must:

- Ensure that you have permission to remove the information from the school by checking your school's protocols and/or procedures or by seeking authorisation from your Line Manager.

- Only take the **minimum amount of information needed**, pertinent to the work that you are undertaking or the visits / meetings you are attending - don't take the entire file and don't take information on the off chance that you might need it.

- In exceptional circumstances it may be necessary for an entire file/record to be removed from the office (e.g. required at a court hearing etc).

- Where an entire file/record is required and is permitted to be removed, senior leaders must implement a simple 'removal log' which records what file/record has been removed from the workplace and when it is returned.

  The log should include details such as:

- **Anonymise** the information or take a summary, which excludes personal identifiers such as name, address, date of birth etc.

- Wherever possible take a copy of the information and leave original in the office (minimise the number of copies in existence by ensuring that you securely dispose of your copy on return to the office).

- Ensure that the information is transported in a suitable bag/briefcase - preferably one which can be locked.

- ✔ Description of the record/file
- ✔ Indicator as to whether the file/record that is to be removed is a copy or the original
- ✔ Reason for removal
- ✔ Name/signature of member of staff removing the file/record
- ✔ Where appropriate, the name/signature of the senior leader who has approved the removal of the file/record
- ✔ Date file/record removed from office
- ✔ Date file/record returned to office
- ✔ Signature of senior leader confirming return

b. Transporting personal information

Reasonable security measures must be made to safeguard personal information whilst in transit. These measures include reducing the visibility of the information to others, and maintaining control of the information at all times.

Remember personal information in paper format is more vulnerable so additional precautions must be taken, such as anonymising documents of the information contained within them.

If your job requires you to visit a number of places during the working day you should carefully consider the risks associated with leaving the information in the vehicle (i.e. risk of vehicle theft/break in etc.) against the risk of taking the information with you, for example into a client's home (risk of the documents being misplaced or left behind when you leave etc.)

If travelling by public transport, personal information will become more vulnerable, and may be susceptible to opportunist crime etc. You must ensure that the information

remains in your possession at all times. Be aware of the risk of theft and ensure that nothing has been left behind when you leave.

£70,000 ICO FINE
London Borough of Lewisham

An employee left sensitive documents in a plastic shopping bag on a train after taking them home to work on.

c. Working with personal information outside school and in a public place

Personal information must not be worked upon in a public area unless it is absolutely necessary.

Be aware of who can oversee the information; pay attention to who is around you, and position your work in such a way that others can't see the content. Work tidily, with care and get into the habit of keeping information discreet.

Ensure electronic devices are fully logged off when not in use and any portable media such as USB memory sticks are removed. Never leave information unattended in a public area or a client's home and always double check that you haven't left anything behind when you leave.

Never ask someone else to photocopy personal information on your behalf when outside of the school environment. If you have to ask someone else to do this for you, always ensure that you are present. Ensure that you retrieve the original document/s from the photocopier and all copies made.

Never dispose of personal information when outside the school or ask someone to do this on your behalf. Take all information back to school and securely destroy where appropriate. (Not primary documents)

d. Returning personal information to the workplace

Wherever possible, personal information must not be retained outside of the workplace or for personal convenience. If this is not practical, the encrypted electronic devices must be stored securely when outside school.

For personal information held in paper format, you must seek permission from your Line Manager to retain the information overnight. If personal information in paper format is permitted to be taken home, **you will have personal responsibility for ensuing that it is kept safe and secure**.

The following guidance must be adhered to if you are unable to return the information to the workplace:

- Never leave information in your car overnight.
- Ensure that all information is taken into your home, hidden from sight and not accessible to anyone who may enter your home including family and friends.
- Keep the information separate from other valuable items in your home.
- Keep information in paper format separate to your laptop.

5. What to do if personal information is lost, misplaced or stolen.

Any loss or theft of personal information, regardless of the format in which the information is held, must be reported immediately to the Headteacher.

Appendix 10 - Schools GDPR Resources – Summary Guidance On Subject Access Requests

---

Data Subjects Rights – Subject Access Requests

An important area of data subjects' rights involves the provision to them of information held by you should they request it. This is called a "Subject Access Request" - (SAR)

As a data controller, the school's response to these requests requires care and consideration in order that timescales are met, that the data subject receives the information they are entitled to, and that where the request may impact upon others, that their rights of privacy are not impacted.

In order that your school is prepared to deal with these requests it is recommended that an individual is nominated to monitor the progress as you respond. This would usually be the data protection officer. This monitoring is especially important where the schools have a large amount of information that may be located in several systems, and in paper and electronic format.

Things to Consider When Dealing With SARs.

- Ensure that your Privacy Notice contains clear details of how to make a subject access request especially the contact details within the school.
- Contact the Local Authority.
- The request can be made verbally or in writing, (email) including via any social media sites the school may use and hold accounts for. If the request is made verbally, it is recommended that you record the detail of the request to avoid any misunderstanding or omission.
- The request may be for information relating to a pupil, a parent or a member of staff.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So, it is important to ensure that you and

your colleagues can recognise a SAR and deal with it in accordance with your school's SAR process.

- It can be made by the parent or older children for themselves and via a third party such as a solicitor acting on behalf of the requester. The requester does not need to specify that it is a SAR.
- If you think an individual may not understand the nature of the information that would be provided to their advocate, or that if they knew the full breadth of it they would prefer them not to know, you may choose to send the information direct to the data subject instead.
- If you have doubts about the identity of the individual you need to validate that the requester is who they claim to be and if it is made by an advocate that they have authority from the data subject.
- The ICO recommends that where a child is mature enough to understand their rights, generally starting around 12-13 yrs, then you should usually respond to the child. A professional would need to decide the maturity level.
- Acknowledge receipt of the request. (once you have validated the right of the individual to make the request)
- Ask early in the process, preferably upon acceptance of the request, in what format and how the requester wishes to receive the information. Paper, electronic – Posted, Email etc. This will mean you have more time to prepare the material in the requested format.
- Generally no fee is chargeable for the provision. However, the ICO does make provision for levying a **"reasonable fee"** where the request is **"manifestly unfounded or excessive"** or where an individual requests further copies following an initial provision. The fee should be based on the administrative costs of producing further copies. If a fee is reasonable, then document how you have calculated its cost.
- The school has 15 school days to respond to a request for the education record of a pupil. This would include: information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body. It may also include information the child has disclosed to you, or from their parent or guardian. Information provided by the parent of another child would not form part of a child's educational record but may still be required as part of the disclosure.

- The timescale for all other requests is one month.
- The ICO considers the first day of the time period to be the day after receipt.
- Make sure that your privacy notice and any public facing material such as a website contains clear information relating to who in the school an individual should contact to request their information.
- If there is any ambiguity in the request, or if it is anticipated that there may be difficulties in providing the information, contact the requester as soon as possible and engage them in discussion to establish whether they may be satisfied with a more specific set of information.
- There is provision to extend the time to respond if the request is complex or the school has received a number of requests from the same individual. If there are difficulties or issues in preparing the information within the timescale, update the requester as soon as you can, and do not wait until the original deadline arrives.
- Start gathering the information as soon as you receive the request, particularly if the request is for a large amount of information and if it needs collation or scanning into the requested format.
- Consider the rights of any third parties who are identified in the information requested. Redact or withhold the information as required.
- Consider any safeguarding or wellbeing issues that may impact a child, the data subject or third parties. For example, this may occur where a parent is requesting information relating to childrens' services referrals or other wellbeing involvements, but there may be other situations. Where required, check with relevant professional teams for their decision on the likely impact.

Appendix 11 - **Good Practice for Avoiding Malware and Other Associated Attacks on School Networks**

More and more of the information used by schools is being held electronically. The benefits are unquestionable, but it can expose an unprepared school to deliberate action that can result in information loss, inappropriate access and fraud.

Acts undertaken by attackers range from covert attempts to breach networks, to manipulation of staff (**also called social engineering*)*** to disclose passwords or to download malicious software onto the network.

Recognising the techniques, educating staff how to avoid them and deploying appropriate system control measures is crucial to reducing the risk of these attacks which are becoming more frequent and sophisticated.

The following are common types of malware.

- Virus: A harmful computer programme that can copy itself and infect a computer.
- Worm: A malicious computer programme that sends copies of itself to other computers via a network.
- Spyware: Malware that collects information from people without their knowledge. (account names, passwords, websites visited etc)
- Adware: Software that automatically plays, displays or downloads advertisements on a computer.
- Trojan horse: A destructive program that pretends to be a useful application, but harms your computer or steals your information after it's installed.

How Malware Can Infect and Spread

- Downloading free software from the Internet that secretly contains malware
- Downloading legitimate software that's secretly bundled with malware
- Visiting a website that's infected with malware
- Clicking a fake error message or pop-up window that starts a malware download.
- Opening an email attachment that contains malware.
- Installing software from memory sticks or other external storage devices.
- Clicking on a link within an e-mail which take you to a malicious website on the internet. (probably the most common these days)

These attacks are commonly undertaken to:

- Gather personal or business data held by the organisation
- Gather data such as passwords, or financial account details that facilitate further access to more valuable systems
- Encrypt and paralyse devices or whole networks and then demanding payment for their unlocking
- Deliver multiple adverts to users and other marketing material
- Gain access to “piggyback” on secure networks to utilise the internet

The following items provide advice on the common areas of risk, but you must take specific advice from your software suppliers and network support providers for information relating to any risks associated with your specific configuration.

The term "**User**" in this guidance covers **anyone** accessing the school's networks.

1. **Install Anti-Virus / Anti Malware Software, Keep It Up To Date and Ensure It Regularly Scans Your Computer(s)\Network.**

   Although seemingly obvious, maintaining a large stock of devices with up to date security can be a challenge, particularly where devices are often stored for long periods and not linked to the network to perform auto updates. Ensure that you have a regime to manage this crucial task

2. **Ensure That The Operating Systems And Applications On Your Devices Are Supported And They Have Been Updated With All the Latest Supplier Patches**

   Many older Windows operating systems are no longer supported by Microsoft, check that all your devices are running supported software. All major suppliers (Microsoft, Apple, Android etc) also issue regular updates which should be applied as soon as they are available.

   The "WannaCry" ransomware attack of 2017 took advantage of PCs that were running old or un-patched Microsoft operating systems, and is estimated to have infected in excess of 200,000 computers in 150 countries.

   Other applications, for instance Adobe Flash regularly update their software and browser plugins.

   Similar to Anti Virus updates, devices that are stored for long periods are likely not have been patched with the latest operating system updates. Ensure you have an effective regime for managing this.

3. **Ensure That All Devices That Connect To Your Network Are Secure**

   The range and types of devices connected to networks has expanded hugely over the last five years. Common devices are Printers, Webcams, Routers and other WiFi devices, external data storage, and very commonly things like smart phones as staff charge them up via USB. Ensure that any that may have default configurations are updated and password protected as necessary.

4. **Ensure All Staff Are Aware Of The Risks Associated With Inappropriate Access To Malicious Websites.**

   Ensure that staff are aware of and have signed your internet access policy, and where possible prevent access to known harmful websites.

   Do not allow the downloading or installing of any applications downloaded from sites without screening by your network support staff.

   Effective use of web content controls can automatically block known malicious sites from being accessed by staff and control access to sites that may be

inappropriate. E.g. Gambling or software download sites. Your network support staff can configure these.

5. **Ensure All Staff Are Aware Of The Risks Of Careless Use Of Email**

Attacks are often experienced via and within the organisations email system, either with links to malicious websites, or with email attachments that deliver software into the network.

The objectives can be varied, and include trying to gain access to data, or trying to fool users into initiating payments on fraudulent accounts etc.

Network and Email security software can be configured to find and block most of these but they need to be updated and monitored. Staff should always be vigilant for emails that appear suspicious and should notify the network support for assistance when something is noticed.

Effective set up and configuration of E-mail Content Scanning tools can automatically detect malicious content and embedded malicious software or attachments. They can also block a large amount of spam e-mails

6. **Ensure All Firewalls And Associated Protection Are Configured Correctly.**

A firewall is a software or hardware based application that helps to block malicious attacks, but they can require effective configuration and management.

7. **Ensure All Of Your Electronic Data Is Securely Backed Up And Undertake Restore Testing**

Should there be a system failure or a malware attack that permanently results in the prevention of access to you your information via encryption, you need to be able to recover your data from tested backups. Many organisations undertake backups without testing them, only to find that there have been problems many months before and the backup is not viable.

Non recoverable loss of data, for instance through hardware failure, that has a significant effect on a data subject, is considered a breach under GDPR and can result in large fines from the ICO.

8. **Enforce The Use Of Strong Passwords To Access The Network And Software Applications**

Users face a growing challenge managing passwords to multiple systems. Without proper password control users can resort to simple, common and repetitive passwords.

Do not record passwords on paper in areas which may result in disclosure. Where your networks and systems can enforce strong passwords (Long and containing numbers and special characters), make sure this is enabled.

9. **Ensure User Accounts Have The Correct Level Of Access To The Network, And That Users Who Leave Have Their Accounts Terminated Appropriately.**

User accounts can usually be granted different level of privilege on the network. Ensure that each account type does not have access to levels greater than required. This can happen when individuals change role and no longer need access to previous applications or data. Ensure you have a procedure for clearing down accounts and closing them for users who leave. Your network administrator will be able to advise you in this area.

10. **Remove Old Applications That Are No Longer Used**

Older, unused or unsupported software can present vulnerabilities on networks. Ensure your network support arrangement include a review of unused software.

11. **Develop and Implement A Response Plan**

Ensure that should an attack be experienced, you have an effective response plan that deals with the attack itself, the recovery of any data and business continuity arrangements should systems be unavailable.

Type of Data	Storage Requirements (Paper)	Storage Requirements (Electronic)	How Sensitive (1 is Low 5 is high)	Special Category Data Under GDPR	Disposal Period	Disposal Method (Paper)	Disposal Method (Electronic)	Disposal Method (email)
Child Protection	Securely, locked cabinet in restricted area.	Password Protected Encrypted drive Server – secure password protected senior staff area.	High - 5	Yes	Up to DOB +75 Years for LAC Pupils Data is transferred securely from school to school. Final school is responsible for final disposal.	Confidential Disposal Shred	Electronic shred of document (not delete) by everyone who holds a copy of that document.	All emails with document attached, even if password protected need to be deleted.
Staff Records	Securely, locked cabinet in restricted area.	Password Protected Encrypted drive Server – secure password protected senior staff area.	Some documents will be highly sensitive.	Yes some documents will be identified as Special Category.	Various up to 15 years from termination for Staff Personal Files	Confidential Disposal Shred	Electronic shred of document (not delete) by everyone who holds a copy of that document.	All emails with document attached, even if password protected need to be deleted.
Pupil Records								

Assessment and Attainment **Examination Results – Primary Schools** **Examination Results – Secondary Schools** **Pupil Progress, Tracking and Value Added (inc CATS) Records – all schools**	Examination results will be held in the schools Management Information System Results will be held in the schools Management Information System	Password Protected MIS Encrypted drive Server – secure password protected senior staff area.	2 2 2	No No No	Current year + 6 years Current year + 6 years	Secure Disposal – **SHRED**	Examination results will be held in the schools Management Information System Information held on personal electronic devises needs to be destroyed within the disposal period.	All emails with document attached, even if password protected need to be deleted.
Governors **Personal data including declaration of business interests**					Generally date of meeting + 6 years		Shred	

General duties of the governing body (minutes etc)								
Actions Required By School	1. Can you identify where all this data is held? 2. Who controls the copies, paper or electronic 3. How do you dispose of the data? 4. What actions do you need to undertake to comply with GDPR? 5. Would you recognise if any of this data had been lost? 6. Who is the data controller? Knowledge and understanding of the above information would be the responsibility of the schools' designated data protection officer. (this is not to be the head teacher to the clerk)							
Things for schools to consider	(Paper) How many copies have been made? Do you know who has a copy? Is there version control of the document? (Electronic) How many emails have a copy of this document? Is there version control? Do you use cloud storage? Is there more than one copy held in the cloud? Who can certify that they are all shredded?							