General Data Protection Regulation Policy

Albright
Education Centre

Sandwell Home and Hospital Tuition Service

Signed by Chair of Governors:	
Date ratified by Governing Body:	12.07.2023
Date of Review:	12.07.2024

1. Introduction – what is GDPR?

The General Data Protection Regulation replaces the Data Protection Act 1998, as of 25th May 2018. This regulation identifies certain principles that any organisation who stores or processes 'Personally Identifiable Information' must be able to demonstrate compliance with. This policy has been out into place to ensure all staff and Governors in the school have an understanding of the scope of the regulation, how it affects them, and the working practices that must be employed on a day to day basis in order to safeguard the personal information of individuals, which we have and use within the school.

2. Applicability

This policy will apply to any member of staff in the school who process personally identifiable information. Such individuals must ensure that they are familiar with the contents and behaviours identified within this policy, and should ensure they refer to this policy when carrying out their duties.

3. Definitions and Common Terminology:

Data Subject: *an identified or identifiable natural person (living)*

Personally Identifiable Information: *any information relating to an identified or identifiable natural person*

Data Controller: *a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.*

Data Processor: *a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.*

Data Protection Officer*: a person who is tasked with helping to protect PII, and helping an organisation to meet the GDPR compliance requirements. Does not hold ultimate accountability for compliance.*

Data Breach: *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data*

ICO: *Information Commissioners Office (Supervising Authority in the UK)*

4. Principles:

In accordance with the obligations placed upon the school as a Data Controller, personal data will be processed in accordance with the Principles of GDPR. The following section lays down how this will happen in practice on a day to day basis.

4.1 Legality, Transparency and Fairness.

Personal data will only be processed by the school, where it is able to demonstrate that it has a 'Lawful basis' for the processing activity.

In order to do this, the school will undertake a data audit to identify and document those data sets / records held within the school, which contain personal information, and in each case, document the lawful basis for processing. Without a lawful basis, processing must not take place, and the personal data should not be held by the school.

The data mapping will be held by the Data Protection Lead and should be considered to be a 'live' document. All staff may be asked periodically to assist in reviewing the data audit to ensure all data sets currently in use within the school have been captured and considered, and a lawful basis for processing identified in each occasion.

The school will endeavour to ensure all Data Subjects are clear about the ways in which the school is processing its personal data. This will include publishing information on the type of personal data being collected, the lawful basis for processing, and types of other organisations who the information is shared with, within a privacy notice.

The Privacy Notice will be made readily available on the school website and paper based copies are available from the school office. A copy of the privacy notice is also included in the schools' admissions packs.

4.2 Purpose Limitation: *personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*

Internal records will be maintained to reflect the purposes for which processing will take place. More specifically, this will be included on the data mapping record, and will include a record of the purpose, description of the categories of individuals and personal data, the categories of recipients of the data (e.g. 3rd party organisations who the School shares the data with); retention schedules for the personal data.

Appropriate technical and organisational measures that must be maintained in order to safeguard data are identified in this policy in general, and will be further documented within Privacy Impact Assessments, if the processing of personal data is higher risk and could result in a risk to the rights and freedoms of the individual (see Appendix 1 Data Protection Impact Assessment for further information on Privacy Impact Assessments).

4.3 Minimisation: *the personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'*

The school will periodically review its' data capture forms and processes, to ensure that the information being requested is not excessive, and that the school is not capturing more personal information than is required.

Personal data collected by members of staff should, wherever possible, be limited to the scope of what is laid out in official school data capture forms. Wherever there is any uncertainty about the level of information being requested from Data Subjects, a referral should be made to the Data Protection Officer for further guidance.

4.4 Accuracy: *every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*

The school shall take proactive steps to check the accuracy of information held within its systems and to subsequently carry out updates as required, through a variety of measures. These include, but are not limited to:

- Issuing data capture forms on an annual basis to parents/Carers to verify the accuracy of personal information held on the SIMS system, including: emergency contact details; correspondence address; medical details of the pupils etc.
- Use of apps such as ParentLite to allow parents real-time access to the above data on SIMS;
- Checking attainment data in systems on a regular basis, through the use of pupil progress meetings;
- Checking accuracy of staff details via amending completion of personal data sheets

4.5 Storage Limitation: *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*

Retention periods for the various records held in the school containing personal data, will be identified and documented as part of the data audit activity.

The school has decided to use the Information Records Management Society Toolkit as its' guide when determining the appropriate retention periods for documents. A copy of this toolkit is available to staff in the shared area (GDPR folder) or via www.irms.org.uk

Archived paper documents are stored in storage wallets clearly marked with the name of the file and year in which it was archived. It also states the date that the documents should be retained until. They are locked in a dedicated storage cupboard which only has 3 keys to open it and are only available to members of the Admin staff and one key is available for Mitie site staff.

Destruction of the documents will be carried out in a timely manner according to destruction dates as advised in the Retention of Records document supplied by IRMS and are then disposed of in Shred-it bins to await disposal. These bins are locked and only Admin staff have access to the keys to open them.

Our contract with Shred-it is for them to collect confidential waste every other month. One of our Admin staff accompany the collector when bins are emptied, tied up and a notification of waste disposal certificate is issued straight away. Copies of these are available upon request.

Electronic documents are kept in encrypted secure shared areas or on Googledrive where a username and password is needed to be able to log in. The password will be regularly updated.

Documents will be stored for the elected retention period (as per IRMS) and marked with a deletion date. Documents will be deleted from the secure area and recycle bins will also be emptied.

4.6 Integrity and Confidentiality: *Personal data will be processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures*

Clear desk and clear screen:

PCs should not be left unlocked when workstations are left unattended. PCs can be locked by hitting ALT, CTRL & DELETE together and clicking LOCK, they also automatically lock after 10 minutes.

Any paper based documents containing personal information should be secured at the end of the day, and when rooms / offices are left unattended. Where there are any concerns over the availability of secure (lockable) storage, or clarification required over the type of information that needs to be secured, staff should in the first instance speak with Michelle Glasgow, the schools' Data Protection Lead, who will liaise with the Data Protection Officer if required.

Positioning of computer screens should be considered carefully to ensure only authorised personnel are able to view sensitive or confidential information. This is of particular importance within areas accessed by members of the public, such as the reception area. Privacy screens will be considered where positioning of screens alone will not address this concern.

Passwords and protection of hardware:

Passwords for accessing systems must be complex enough to make it extremely difficult for third parties to break them: passwords should be at least 8 characters long, have a mixture of upper case and lower case letters, at least one number and one character.

Passwords should be changed regularly, and never shared with any other member of staff / shared amongst other users.

Mobile devices (including phones, tablets and laptops) must be protected to the same high standard. You must:

- Activate the built in security PIN and set this to the most secure level (if the device allows, this should always be a secure password as detailed above or fingerprint recognition rather than a 4 digit pin;
- Ensure that you have a copy of IMEI numbers for the phone and the SIMS stored securely to allow deactivation in the event of loss.

You are personally responsible for any information accessed or disclosed on these devices so it is imperative that you keep your password safe and secure, and do not share it with anyone else.

Accessing and sharing information:

There are many different ways in which School staff can access data. It is their responsibility to know if they are simply accessing the data that is stored securely elsewhere, or downloading or saving data to a School device. Office 365 and the tools it provides allows employees to not only access their emails but actually open, modify, save and /or send any data that is held.

It is important that employees understand the difference between accessing data (looking at or reviewing) via a mobile or off-site device and downloading/Saving data (this will save a copy of the information onto the mobile device you are using) to a mobile or off-site device. Data should not be downloaded or saved to a mobile or offsite device unless you can justify this action with a clear business case for doing so. Once the data is no longer required on the device it must be deleted immediately*.*

There are also times when it will be necessary to share information with others.

Inside the School:

- When sharing information with others within the School, if information is of a confidential, sensitive or personal nature, it must be treated as such. Information should only be shared with the individuals who require it, do not copy people into emails if they do not require access to the information contained within. Delete sensitive, confidential or personal information once it has been used for the purpose it has been collected and is no longer required.

Outside the School:

Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods can be used. If in doubt please check with the Data Protection Officer.

- Secure transmission: Where possible, use recognised secure transmission methods such as WebEx.
- Never send personal data within a normal email. If email is the only method of transmission available, ensure the information is included in a password protected document. The password must be agreed with the email recipient in advance, and via telephone, not in another email. Never include the password in the email to which the password protected document is attached, nor send the password via another email (if the first email is intercepted, then the second could also be).
- Ensure that the request for data is a valid one and that only the required data is provided. Always check why people require the data they ask for – if in doubt check with the Data Protection Lead before sending.
- Make sure that the data is up to date. Check the accuracy of the data to be sent before sending
- School Emails should never be sent to public email addresses (e.g. Hotmail, Gmail etc.) regardless of what they contain, unless this has been clearly identified by the recipient as their business email address.

When sending information (including letters) via post the following must be adhered to:

- Always get a second person to check the address is correct before sending. Pay particular attention to numbers as these are easily transposed, however, be aware the responsibility for the accuracy is still with the Sender not the Checker

- Always use window envelopes if the address is pre-populated on the enclosed letter to avoid transcription errors or typed labels to avoid issues in relation to legibility of handwriting.
- Always ensure that envelopes are securely sealed. Use additional methods such as sticky tape, glue or staples if deemed necessary
- Double check that no additional information has been included that is not relevant e.g. something mistakenly attached. Only send relevant data. Check that it is valid and accurate and no additional information i.e. additional sheets are included in error.
- If a request is received from an outside agency such as the Police, this should be referred in the first instance to the Data Protection Lead.

Storage of Data on Portable/External Devices

- The loss of any device that can send, store or retrieve data must be reported to your Data Protection Lead and the Data Protection Officer immediately.
- Devices that are capable of transmitting and receiving data information, such as smartphones, should only be used for the purposes for which they were supplied and must be protected by a strong secure password.
- Anyone who uses portable devices to access or store data is responsible for the information which is transported within. This includes USB flash memory devices ("memory sticks"), laptops, external hard disk drives, mobile phones, tablets. Be aware of devices that can access information, such as emails, that could contain sensitive data.
- Any memory stick/portable device that you use for the transport or storage of personal or sensitive nature must be encrypted to an appropriate standard and approved for use by our Data Protection Lead / IT Support. All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information must not be written down and must never be stored or transported with the device. Please be aware an encrypted memory stick/portable device will ALWAYS ask you for a password before use.
- Any storage devices no longer required which may contain information that is surplus to requirements or any device that is in need of secure disposal should be returned to our IT staff or the Data Protection Lead, in person.
- Media such as CDs or DVDs which contain data and are no longer required must be physically destroyed. If you do not have the means to do this, please pass them to the IT Department/Data Protection Lead for disposal – stating clearly that they contain sensitive information
- All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information must not be written down and must never be stored or transported with the device.

Please see Appendix 2 Online Safety Policy and Appendix 3 Acceptable Internet Use

Paper and Manual Filing Systems

Paper based (or any non-electronic) information must be assigned an owner. A risk assessment should identify the appropriate level of protection for the information being stored. Paper and files in the School must be protected by one of the following measures:

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

It is important that someone has ownership i.e. takes responsibility for the storing and protecting of such systems.

Security of Equipment and Documents Off-Premises

Information storage equipment, data, software or any documents containing personal, sensitive or confidential data should not be used off-site without authorisation from the Head Teacher.

Information storage equipment includes items such as personal computers, organisers, PDAs, tablets, mobile phones and external storage devices.

The following security guidelines must be adhered to for all equipment and documents taken offsite, it must:

- not be left unattended in public places.
- not be left unattended in a vehicle unless the property is concealed from view and all doors are locked, windows and the roof closed and fastened, all security devices on the vehicle are put in full and effective operation and all keys/removable ignition devices removed from the vehicle
- not be left open to theft or damage whether in the office, during transit or at home
- where possible, be disguised (e.g. laptops should be carried in less formal bags)
- be returned to the School as soon as is practically possible.
- Where it is necessary to transport sensitive or personal data in this manner, data encryption must be in place, and manufacturer's instructions for protecting the equipment should be observed at all times

Physical Security

Our data must be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. This section is related to building security and the level of care that you are expected to provide when transporting computers or paper files outside of the building.

- Our premises are protected by door locks and access codes. It is important that the codes remain secure as these form part of our physical security procedures and as such help to keep our personal, sensitive and confidential data safe.
- Doors and windows must be locked when unattended and external doors (including loading bay/fire doors) must be locked when not in use.
- All visitors must sign in and receive a Visitor's Authentication Badge. This is issued by the staff in Reception and applies to all Visitors.

- All Visitors/Attendees should be supervised at all times and are required to wear visible authorised identification, and to record their date/time of entry/departure and person(s) being visited.
- Confidential data or computer systems that contain such data. If such access is requested, it is the employee's responsibility to ensure it is a legitimate request and data protection is not breached. If in doubt, please check with your Data Protection Lead or the Data Protection Officer.

4.7 Accountability – *the Controller will be able to demonstrate compliance with the previous principles.* The school will do this by employing measures including:

Ensuring a Data Protection Officer is appointed. This individual will have suitable knowledge and experience to fulfil this role and will have a direct line of report through to the Head Teacher and Governing body for data protection related matters.

On a day to day basis, the first point of contact within the school is the data Protection lead (Michelle Glasgow); the Data Protection lead will liaise with the Data Protection Officer for advice and guidance as required.

The DPO will undertake periodic monitoring activities to help ensure compliance with the regulation. They must be informed of any suspected data breach, and will help to investigate circumstances surrounding breaches, and ascertain whether they are required to be reported to the ICO.

The DPO must also be informed of any Subject Access Requests that are submitted to the school, and will assist in making the response to the Data Subject.

For our school the Data Protection Officer is Sue Courtney-Donovan, SIPS Education, and are contactable via gdpr@sipseducation or 0121 296 3000.).

Our Governing Body will be kept informed of our ongoing compliance via reports to Mary Parkes, Chair of Governors which will include an overview of any data breaches that have occurred along with actions taken, and any Subject Access Requests received and responded to.

Training for staff and Governors will be provided by the DPO on an annual basis, and further supplemented by reminders in school on policy and procedures to follow to safeguard personal data.

Where the school needs to share personal data with 3rd party organisations (Data Processors), it will ensure that adequate steps have been taken to vet the robustness of the Processors systems in order to safeguard the information shared, and will maintain a written record of this.

Data Protection will be considered as part of all project planning, when we are reviewing our systems for data collection and data processing. Where required, we will undertake Data Protection Impact Assessments to ensure appropriate measures are put in place to safeguard the data, prevent breaches and ensure compliance with the requirements of the Regulation. A copy of the Data Protection Impact Assessment is included at Appendix 1.

5 The rights of the Data Subject

Under the Regulation, Data Subjects have 8 rights, as listed below. The School will ensure procedures are in place to be able to respond in a timely manner to any request from a Data Subject to exercise one of their rights. The Data Protection Lead in the school will liaise with the DPO as required, to ensure an appropriate response.

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

6 Subject Access Requests

If a data Subject wishes to see copies of the information held on them by the School, they may submit a Subject Access Request. Such requests must be made in writing in order to be valid. Any such requests received by members of staff must immediately be forwarded to the Data Protection Lead who will liaise with the DPO in order to make the response. No member of staff may divulge personal information over the phone, or respond to such a request without the express consent of the Data Protection Lead.

Responses to SARs must normally be made within one month, so it is imperative that such requests are brought to the attention of the Data Protection lead without delay. A further 2 months may be used in exceptional circumstances only, and only with the agreement of the DPO.

Procedures for Responding to Data Breaches

If any member of staff becomes aware of a data breach situation, they must ensure this is reported to the Data Protection Lead as soon as possible. The school is obliged to keep a record of all breaches and investigate them to an appropriate level, in order to ascertain what can be learnt from the circumstances surrounding each, and then used to review procedures as required with the aim of preventing a similar breach occurring again.

Some breaches of a more serious nature will need to be reported to the ICO. The DPO will help the school to ascertain whether a breach is reportable, and will advise on all such occasions if this is the case. The Data Protection Lead will liaise with the DPO to determine whether a breach is reportable or not.

Where breaches are reportable, the report must be submitted to the ICO within 72 hours of the school becoming aware of the breach, and so it is crucial the Data Protection Lead is notified of any potential breaches immediately.

You must also report any near misses so that we can learn from these also, and use them as a way of informing future revisions to our policies and/or procedures for data protection.

Appendices:

1. Data Protection Impact Assessment
2. Online Safety Policy
3. Acceptable Internet Use Policy

Albright
Education Centre

Appendix 1

Data Protection Impact Assessment Template

Data – Electronic or Hard Copy	Current Process	Impact of threat if occurs: 1 = low 5 = High	Likelihood: Low, Medium, High	Steps Taken to Minimise Risk	Action Plan/Next Steps	Review Date

Appendix 2

Online Safety Policy

Albright
Education Centre

Sandwell Home and Hospital Tuition Service

Signed by Chair of Governors:

Date ratified by Governing Body: 08.02.2023

Date of Review: 08.02.2024

Attachment & Trauma Aware School ACEducation

Positive About Disabled People

Ofsted Outstanding 2009|2010

Ofsted Outstanding School 2012|2013

the sandwell well-being charter mark

Rationale

It is the duty of the service to ensure that every child and young person (CYP) in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, CYP are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: Child Protection, Health and Safety and Behaviour.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by pupils or staff.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements in this service:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive e-Safety education programme for pupils, staff and parents.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this service and the Head Teacher, with the support of governors, aims to embed safe practices into the culture of the service. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis. The responsibility for e-Safety has been designated to a member of the senior leadership team.

Our school **e-Safety Coordinator is Stephen Downey**

Our e-Safety Coordinator ensures he keeps up to date with e-Safety issues and guidance through liaison with Broadband Sandwell's e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). The school's e-Safety Coordinator ensures the Head, Senior Management and Governors are updated as necessary.

Staff awareness

- All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.
- New staff receive information on the school's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.

- E-safety records of concern are completed by staff as soon as incidents occur and are reported directly to the school's designated safeguarding team.

All staff working with CYP are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Internet:

- The service will use Broadband Sandwell "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material.
- Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.
- Staff should email school-related information using their school account and not their personal accounts.
- Staff will preview any websites before recommending to pupils.
- Internet searches are conducted using the Safe Search homepage found at http://www.safesearchkids.com/.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator(s) detailing the device and username. Agilisys can then be informed and contact to TrustNet can be instigated.
- Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and then Agilisys so that the Service Provider (TrustNet/Virgin Media) can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- Pupils will be asked to sign to the Acceptable Use Agreement thus ensuring that they are aware of expectations. Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Mobile technology for pupil use, such as iPads and netbooks, are stored in a locked cupboard. Access is available via the school office, keyholders or Agilisys. Members of school staff (not visitors or children) should sign in/out the technologies before and after each use.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- Should personal devices be used to take pictures or videos of pupils (for example on trips) once downloaded onto the school system, all traces should be deleted off the personal device.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or children are to be used during the school day. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent. If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept switched off and handed in to the school office during the school day, and will remain the responsibility of the child in case of loss or damage. Any pupil not following these rules will be dealt with using the school's behaviour policy.

Data storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Google Drive Account.
- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Management Team.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply. This could also undermine any complaints procedures.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the Service into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

The Service reserves the right to monitor staff internet usage. The Service considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

Digital images

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children unless prior authorisation has been provided. If it is used in this way then images must be removed before leaving the school premises.

- Ensure you are aware of the children whose parents/guardians have **not** given permission for their child's image to be used in school. An up to date list is kept in the school administrative office.
- When using children's images for any school activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-safety education to pupils and parents

- All staff working with children must share a collective responsibility to provide e-safety education to pupils and to promote e-safety in their own actions.
- Formally, an e-safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if e- safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.
- Informally, a talking culture is encouraged in classrooms which allows e-safety issues to be addressed as and when they arise.
- The ICT Coordinator will lead an assembly twice a year, including on Safer Internet Day, highlighting relevant e-safety issues and promoting safe use of technologies.
- eSafety themes are also woven into the fabric of the centre curriculum.
- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's ICT guidelines.

Maintaining the security of the school IT Network

Agilisys maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network Complaints procedure.

As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be recorded using a Notice of Concern proforma and reported to the school's designated safeguarding officer in accordance with school's child protection policy. Complaints of

Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

The Head Teacher/Deputy Head Teacher or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Lead.

Appendix 3

Albright Education Centre

Acceptable Internet Use Policy Statement (for ALL Staff)

The computer system is owned by the school. This Responsible Internet Use statement helps to protect staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- Users should log off or lock the computer when leaving a workstation, even for just a short period.
- School computer and Internet use must be appropriate to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of unauthorised chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the Head Teacher has given permission for that use.

- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials. Such action may be taken where the school believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

This policy is to protect the interests and safety and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policy: Online Safety.

This Acceptable Use Policy (for all staff) is inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by staff.

✂………

Acceptance of the above conditions

Full name: ____

Signature: ____

Job Role: ____

Date: ____