The Evolution and Henslow School

GDPR, Data Protection and Information Sharing Policy

Contents:

General Data Protection Regulations

Introduction

The UK Data Protection Act 2018 (DPA 18)/UK GDPR defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.

Reflexion Care Group Limited; including the trading names including but not limited to New Reflexions and New Reflexions Education are committed to protecting the privacy of individuals and handle all personal information in a manner that complies with the DPA 18. It is the **personal responsibility** of all employees (temporary or permanent), members of the board, contractors, agents and anyone else processing information on our behalf to comply with this policy.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the UK DPA/UK GDPR 2018. All breaches will be investigated, and appropriate action taken.

This policy explains what the Company's expectations are when processing personal information. Please also refer to our School information security policy.

GDPR Principles

The UK DPA/ GDPR 2018 is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

These principles state that personal information must:

Be processed fairly, lawfully and transparently	Obtained for a specified, explicit and legitimate purpose	Be adequate, relevant and limited to what is necessary
Be accurate and where necessary up to date	Not be kept longer than is necessary	Be handled ensuring appropriate security

Access and Use of Personal Information

Access and use of personal information held by the Company, is only permitted by employees (temporary or permanent), members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

Collecting and displaying Personal Information

When personal information is collected, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice. Our Privacy Notice can be found on our school website - https://www.reflexionseducation.org.uk

The school does not collect any biometric data e.g. personal information about an individual's physical or behavioural characteristics that can be used to identify that person, such as fingerprints, facial shape, retina and iris patterns, or hand measurements. The school does use CCTV for security and monitoring purposes, **please see further information in our CCTV policy.** Any enquiries about the CCTV system should be directed to the Head Teacher.

Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see below). It must be made clear to the 'data subject' all the purposes that their information may be used for at the time the information is collected, via a Privacy Notice.

Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards or posters and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Lawful Basis for Processing

When we process personal information, we will have a lawful basis for doing so.UK DPA/ GDPR 2018 provides a list of 'conditions' when we can process personal or 'special category' personal information. This is contained within Article 6 and Article 9 of the Regulations, see Appendix 1.

The UK DPA/UK DPR 2018 defines special category personal information as information relating to:

- race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition;
- sexual life

Whenever we process personal information, it must be able to satisfy at least one of the conditions in Article 6 of the UK GDPR and when we process 'special category' personal information; it must be able to satisfy at least one of the conditions in Article 9 of the UK GDPR as well.

We can process personal information if we have the data subject's consent (this needs to be 'explicit' when we process sensitive personal information). In order for consent to be valid it must

be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded. All adults in school will support learners to ensure they understand consent before signing.

Disclosing personal data/information

Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

If personal information is given to another organisation or person outside the company, the disclosing person must identify the lawful basis for the disclosure. They should ensure there is a clear trail of this sharing which indicates:

- the information given
- the name of the person and organisation the information was given to
- the date
- the reason for the information being given; and
- the lawful basis

The school's approach to information sharing is detailed in this policy and will be adhered to when providing personal information to others and will provide the legal basis for disclosure. Where there is defined justifiable purpose, the school will sign up to information sharing agreements with partner organisations, where these agreements are within the boundaries of applicable legislation and regulation and do not compromise the school or the confidentiality of the personal and/or sensitive data that it holds. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

In response to any lawful request, we will provide only the minimum amount of personal information. The person giving the information should make sure that it is adequate for the purpose, relevant and not excessive. When personal information is given either internally or externally, we ensure that it is communicated in a secure manner e.g. password protected, encrypted emails, sent by a trusted courier service etc

Accuracy and Relevance

It is the responsibility of those who receive personal information to make sure so far is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure it is still relevant and up to date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

'Data subjects' have a right to access personal information held about them and have errors corrected. More information about a data subject's rights can be found later in this policy under individual rights.

Retention and Disposal of information/records

The company holds personal information. The UK DPA/UK GDPR 2018 requires that we do not keep personal information for any longer than is necessary.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Generally complete school records will be maintained until the student reaches 25 years of age. Please refer to our records management policy for further details.

Individuals Rights

Individuals have a number of rights under the UK DPA/UK GDPR 2018. These include:

- **The right to be informed** – See section 4 - Collecting Personal Information
- **The right to access** – A person can ask for a copy of personal information held about them (this is known as a Subject Access request - SAR);
- **The right to rectification** – Personal data can be rectified if it is inaccurate or incomplete
- **The right to erasure** – Person can ask for the deletion or removal of personal data where there is no reason for its continued processing
- **The right to restrict processing** – Person has the right to block or suppress processing of their personal data
- **The right of data portability** – Allows a person to obtain and reuse their personal data for their own purposes
- **The right to object** – A person can object to an organisation processing their personal data for direct marketing, on the basis of legitimate interests or for scientific/historical research and statistics
- **Rights related to automated decision making/profiling** – A person can ask for human intervention in an automated process

If the school receives such a request on any of the above matters they should seek advice from their Data Protection Officer as soon as the request is received.

The school has one calendar month in which to respond to a SAR, provided the applicant has clearly stated the nature of their request preferably by completing a subject access request form and suitable proof of identification has been supplied. However, the law does allow a SAR to be made verbally. An extension of a further 1-2 months will be applied where a request is deemed

complex, the requester should be informed of this within one month of the request being received. The school and Data Protection Officer co-ordinates the processing of all SAR requests. ***See Appendix 2*** for a copy of the SAR form.

Reporting Security Incidents

The school has a responsibility to monitor all incidents that occur which may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported on a timely basis, investigated and monitored. It is only by adopting this approach that the school can learn from its mistakes and prevent losses recurring. The Data Protection Officer must be informed of an incident/breach within 24 hours of the school becoming aware of the matter.

Specific procedures have been developed for the reporting of all information security incidents. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. The documents below need to be read, understood and followed:

- Information Security Breach Procedure
- Data Breach Investigation

All employees (permanent, temporary and contractors) must be aware of the procedures and obligations in place for reporting the different types of incidents which may have an impact on the security of the school's information. See Appendix 3.

Data Protection Officer

As the school is a public authority, it has a legal duty to appoint a designated Data Protection Officer.

The Data Protection Officer has a number of legal duties that they must fulfil including:

- Inform and advise the school of its obligations in respect to data protection
- Monitor compliance with data protection legislation including awareness raising and training of staff
- Provide advice on data protection impact assessments
- Be a contact for the Information Commissioners Office

The schools current designated Data Protection Officer is Rob Montgomery/Sarah Daffern. Sarah.Daffern@telford.gov.uk, Robert.Montgomery@telford.gov.uk

Accountability

The DPA 18 requires the school to have appropriate measures and records in place to demonstrate compliance with the act.

The school demonstrates accountability in a number of ways including:

- Having appropriate policies in place
- Following data protection by design and default
- Using data processing agreements in contracts
- Maintaining records of processing activities
- Implementing technical and organisational security
- Managing data breaches
- Completing data protection impact assessments
- Having an appropriately skilled and knowledgeable Data Protection Officer

Training

All school staff are provided with data protection training as part of their induction process to ensure that they are aware of their responsibilities.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Staff will be updated regularly through:

- ❖ Dissemination of emails from the DPO
- ❖ Ongoing email reminders about key policies such as the schools Data Protection Policy updates as well as the Information Sharing Policy and Information Security Policy.
- ❖ Email reminders on preventing data breaches
- ❖ Disseminating lessons learned to all staff if the school does experience a data breach or examples from the press.
- ❖ Accessing additional training where appropriate

Reviewed by:	J Brooks	**Date:** January 2024
Last reviewed on:	August 2023	
Next review due by:	January 2025	

Article 6 Conditions – Personal Data

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **This shall not apply to processing carried out by public authorities in the performance of their tasks.**

Article 9 Conditions – Special Category Data

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and

services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2

UK Data Protection Act/ UK General Data Protection Regulations 2018
Right of Access to Personal Data

SUBJECT ACCESS REQUEST FORM (SAR)

Information

We should respond to your request within one calendar month. Note this can be extended for a further 2 months if the request is deemed complex. However this period does not start until:

a) We are satisfied about your identity
b) You have provided enough detail to locate the information you are seeking

Please complete the following sections of this form providing as much information as possible to help us deal with your request.

1. Provide details of the person(s) about whom the school is holding data (the Data Subject)

Full Name (Print) _____

Date of Birth _____

Present Address:	Previous Address (if less than 3 years at your present address):
Post Code:	Post Code:

Telephone Number _____

Email address _____

2. Are you requesting information about yourself (person referred to in question 1)? If **YES**, then go to question 3. If **NO** please complete the following:

Full Name (Print) _____

Present Address:

Post Code:

Telephone Number: _____

Email address: _____

Relationship with data subject and brief explanation as to why you are requesting this information rather than the data subject:

_____

_____

If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject (see section 4 for details of acceptable identity)

3. Please provide a clear description of the information that you are requesting, see table below. **If you provide <u>specific</u> details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.**

Description of Information	School Staff Member Holding this Information	Time Period for Information Requested

4. Please provide **two** pieces of evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.

Driving Licence	Passport	National ID Card	Medical Card	Utility Bill

You may wish to send your documents special/recorded delivery. Your proof of identity will be returned to you securely after verification.

5. All information in respect to your request will be sent to you via secure email unless alternative arrangements are made. We may require further evidence of your identity if you collect your information from school premises.

Declaration

To be completed by all applicants. Please note that any attempt to mislead the school may lead to prosecution.

I (insert name) _____

certify that the information given on this application form and any attachments therein to The Henslow and Evolution School is accurate and true.

I understand that it is necessary for the Henslow and Evolution School to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.

Signature _____

Date _____

Return of the Form

If you are either posting your documents or hand delivering them then our address is detailed below:

The Henslow and Evolution School, Middletown, Nr Welshpool, Shropshire, SY21 8FF.

Our email address is admin@reflexionseducation.org.uk

Please read before filling in the Subject Access Request Form

Which sections should I complete?

Sections 1, 2, 3, and 4 should be completed for all applications.

Sections 5, 6 and 7 (Representative Details and Authority to Release Information to a Representative) should only be completed if the application is being made by a representative (i.e. someone other than the data subject themselves).

What information will help with the processing of my subject access request?

If you cannot provide us with satisfactory proof of identity, your application will be rejected

What information does Reflexion Care Group Limited hold?

Reflexion Care Group Limited only holds information relevant to enable it to conduct its business and to meet its legal obligations, which will include, but is not restricted to, personal information about employees, contractors, customers and young people. Please note that some data may have been reviewed and destroyed where appropriate in accordance with information retention guidance.

Reflexion Care Group Limited is the 'data controller' for certain information held on behalf of certain third parties who contract to Reflexion Care Group Limited who provide certain

How long will it take to get my data?

Once we are satisfied that you meet the criteria for disclosure of data under the Data Protection Act, and have provided sufficient information, you should receive a response within 30 days from the date that we accept your application for processing.

Records may be held in several different locations in paper and electronic formats, in complex cases this timescale may need to be extended, if this occurs you will be informed in writing. If you only require specific information and you clearly state what that is – for example a specific document or IT-only data – then you are likely to get a quicker disclosure.

The form includes a section for giving details if you need a disclosure by a certain date. No guarantee can be given that a disclosure will be completed by that date but we will endeavour to comply with reasonable requests for expedited action.

General Notes

1. We will not acknowledge your application in writing but we will provide you with a reference number when we write to you.
2. Subject access requests from parents or carers of children may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.
3. The documents that you receive may have data redacted (blacked-out) or contain rough notes that may lack clarity. This is because we aim to supply copies of the original records whenever possible. However, certain records may also include third party information which we cannot release to you under the Data Protection Act, e.g. another person's data, this is removed.
4. We will not disclose information by fax or telephone. Disclosure by post is usually made by first class post to the address you provide in section 2 or, if appropriate, to your representative named in section 5.

Checklist

☐ Have you completed all relevant sections of the form?

☐ If you are a representative, has your client signed the authority in Section 7 or provided a separate signed note of authority?

☐ If you are submitting the form yourself, have you signed the form at Section 4?

☐ If you are signing as a parent or guardian of a child under 16, have you provided a photocopy of their full birth certificate, photocopies of any court orders and proof of your parental responsibility?

☐ If you are a Representative have you enclosed two pieces of identification from the lists in Section 6 (one from each of A and B)?

☐ Have you signed the declaration in Section 4?

☐ Have you provided as much information as possible to enable us to find the data you require?

Please send your completed form and any proof of identity required to:

HR manager

Reflexion Care Group Limited

Cruckton

Shrewsbury

SY5 8PR

Tel: 01939 210040

Email: HRadmin@newreflexions.co.uk

What to do in the event of a possible data breach/incident

1. Introduction

1.1 This procedure details the necessary steps to take if you have concerns that there has been a breach of personal identifiable information (PII) by New Reflexions employees, members or third parties contracted to provide services.

1.2 Some typical examples of a data breach include, but are not limited to:-

- **Personal Data –** e.g. name; address; telephone number; date of birth; NI number; bank account details
- **Sensitive/Special Personal Data –** e.g. information specifically relating to physical or mental health or condition; race or ethnicity; political opinions; religious beliefs, or beliefs of a similar nature; membership of a trade union or non-membership; sexual life; commission or alleged commission of an offence;

2. What is a possible data breach?

2.1 A breach is where identifiable personal information has been or has the potential to be:

- Viewed or copied by an individual unauthorised to do so,
- Communicated to an unauthorised individual/organisation, e.g. sent to wrong address and opened/read
- Lost or stolen

There are many examples of what constitutes a possible data breach, typical examples are detailed below:

- Loss of mobile phone/laptop or other ICT equipment
- Personal information being emailed/posted/faxed to an unintended recipient or address and read by the individual.
- Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personal grant information
- Not keeping information secure; i.e. leaving correspondence on your desk at the end of the working day

2.2 There may be security incidents where Personal data has been given to an unauthorised person (due to a human or procedural error) but the recipient has not opened/read the data. The data has then been returned or it has been confirmed that it has been destroyed. Cases such as these should be notified to the Head Teacher who will be expected to undertake their own investigation into the security incident and implement actions that will minimise the possibility of a similar incident in the future.

3. What should I do if I become aware of a possible data breach?

3.1 Outside a normal working day

3.1.1 If you become aware of a possible data breach you should report it immediately where you can. If this occurs outside normal working hours, e.g. bank holidays, weekends, etc., please contact your line manager within 24 hours of the incident occurring.

3.2 Normal working day

3.2.1 If a breach occurs or you suspect one has occurred you will need to inform your line manager (who will inform the relevant people; including but not limited to the HR manager and DPO service). The matter must be forwarded within 24 hours of the incident occurring for recording and investigation.

3.2.2 If the incident involves theft or a crime then your line manager (Head teacher) should contact the police and report this. Please make sure you obtain and record a crime reference number from the police where applicable.

3.2.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with the IT manager.

3.2.4 When the matter is reported the following information as a minimum should be to hand:

- Crime reference number given to you by the police (if applicable)
- Police station and constabulary the incident was reported to (if applicable)
- Place, time and date(s) the incident occurred
- Employee and/or team(s) details or 3rd party suppliers involved
- A summary of the information that has been lost, stolen or incorrectly communicated
- A list of the individuals affected or that could be at risk
- A list of organisations that may need to be contacted (e.g. shared service information), if applicable
- Confirmation as to who else in the authority has been informed

3.2.5 When the incident is reported to the Head Teacher they will:

- Assess the level of the risk associated with the incident
- Agree the immediate mitigating actions that should take place and who should undertake them including who else needs to be informed (internally and externally)
- Agree who will undertake an investigation into the incident –
- Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the Directors) if applicable
- Produce or agree the production of a report
- Agree remedial action to be taken
- Communicate any lessons learnt corporately where appropriate

DATA BREACH REPORTING FORM

	Report prepared by: Date	
1	Summary of the event And circumstances	
2	Type and amount of personal data	
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	
	Breach investigated by: Date:	
5	Procedures / instructions in place to minimise risks to security of data	
6	Breach of procedure / policy by staff member	
7.	Measures already taken to address the breach.	
8	Details of notification to affected data subject Has a complaint been received from Data subject?	
9	Details of Data Protection training provided	
10	Procedure changes to reduce risks of future data loss	
11.	Description of actions taken against the officer implicated in the breach. (if any)	
11.	Lessons learned to be implemented (if relevant)	

SUMMARY GUIDANCE – Record Management and Security Policy

'Information security is everyone's responsibility'

This is a summary of the School record management and security policy . A full version can be located within the School Policies and Procedures.

1. Why do we need security?

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post, email, and even spoken in conversations.

The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level from events that may cause personal distress or have a negative impact on the School and its services.

This policy promotes good practices in respect to information security ensuring 3 main principles are embedded in the authorities' manual/electronic records management systems:

Confidentiality	Integrity	Availability
Information only accessed by authorised individuals	Safeguards accuracy and completeness of information	Ensure authorised officers have access when needed

Information security is not all about protecting the School from financial penalties it is about respecting the lives and rights of the residents/partners in our community and our employees.

2. Lost Information

You should always report any instances of lost personal information or where it has been sent to the wrong person(s) immediately to the Head Teacher so the risks and impacts can be properly managed. Do not forget information security concerns many things including letters, reports, emails, paper files, etc, but can also include issues such as lost laptops, work mobile phones, lost digital cameras, lost memory sticks, etc. See the Information Security Breach Procedure (ISBP) in the staff handbook.

3. Sharing Information

What should you consider when asked to share personal identifiable information (PII) with other third parties?

- Only share PII if you have the legal justification to do so
- Share information in compliance with the Information Sharing Policy
- Know the objective/reasons for sharing PII
- Investigate whether the objective can be met another way without sharing PII
- Send elements of PII that are definitely required to meet the objective/reasons
- Where possible, anonymise the information you send so it is not personally identifiable
- Confirm the recipients contact details before sharing information
- Appropriately protect the PII you are sharing by either using encryption / password if it is electronic, by using special delivery if posting, etc.

4. Sensitive Information

The School handles numerous types of sensitive data on a day-to-day basis. The following are a list of do's and don'ts in respect to handling sensitive data.

Do's	Don'ts
If you lose any sensitive or personal information then this should be reported immediately to your Head Teacher	Do not store sensitive or personal information on portable media (laptops, memory sticks, CD's, etc) unless in very exceptional circumstances and when the media is encrypted
When discussing sensitive or personal information on the phone consider who may be listening in at both ends of the phone line	Do not give out sensitive information unless the person is authorised to receive it and the data owner has approved that you can send it
Understand your responsibilities under the UK Data Protection Act 2018	Do not leave sensitive or personal information on printers, computer screens or desks whilst away from your desk
Keep sensitive information stored securely and restrict access on a need to access basis	Do not access any sensitive or personal information that is not relevant to your role
Ensure that sensitive data, both paper based and electronic are shredded / disposed of correctly	

5. Passwords

It is your responsibility as a user to:

- Do not share passwords
- If you think someone is aware of your password change it straight away
- Avoid writing down passwords
- Make passwords hard to guess; try to avoid using family names.
- Change your password every 3 months or when prompted to do so.

6. Email/Other Communication Technologies (OCT)

Appropriate use includes:

- Email/OCT (private on School equipment) must not contain indecent, inappropriate or offensive content
- Take care when addressing email messages to ensure a correct address is used
- Do not send personal or sensitive information via unprotected email
- Reasonable personal use is allowed in non-work time only
- Do not take part in chain letter emails

7. Internet

You should always remember that your School internet access is primarily provided for business use. See The record management and information policy for what is defined as reasonable use of the internet. Please note:

- All internet use on School equipment is logged for management purposes
- Reasonable personal use is permitted in non-work time
- Do not use the School's internet (both within and outside working hours) to access inappropriate, offensive, illegal or adult/sexually explicit material.
- Do not leave the internet logged on when you leave your computer unattended

8. Summary of Key Messages to Employees

YOU MUST:

- Ensure you take steps to safeguard the security of information you hold/access
- Comply with the acceptable use policies and the information breach procedure
- If you handle personal information, have an adequate awareness of your UK Data Protection Act/GDPR responsibilities
- Report lost/stolen ICT equipment/personal information to your Head Teacher
- Complete information governance training
- Only share personal information if there is legal justification to do so
- Where possible anonymise personal information shared with non-School parties, e.g. use a reference number and not a name
- Appropriately protect information that is being shared
- Confirm the recipients details, e.g. email address, location, etc. before sharing the information
- Only access information/systems that you need to undertake your duties

- Use secure passwords and never share them with your colleagues
- Direct external parties that need access to the School's network to the ICT Technician
- Lock down your pc/laptop when you leave it unattended for a prolonged period
- Be responsible for the physical security of School ICT equipment and information in your possession (i.e. paper files) making sure that these are securely stored
- Ensure your mobile device has PIN security activated
- Only use USB sticks or other removable media (e.g. external hard drives, digital cameras, etc) on an exception basis and only use those that are encrypted
- Ensure information held on removable media is encrypted/password protected
- If you are mobile/home worker, ensure that ICT equipment and information used on the road or at home, is locked down/away securely when not in use
- Never leave ICT equipment and/or personal information in a car overnight
- Do not use email on School equipment/networks for personal use in works time
- Only use the internet for personal use in non-work time
- Undertake a data protection impact assessment on all new/developed ICT systems that involve processing/viewing of personal information