GDPR Policies

Date approved: - Spring Term 2020

Date to be reviewed: - Summer Term 2021

Governing Body Committee: - Full Governors
Contents

- Data Protection Policy Page 3
- Statutory Request Policy Page 8
- Acceptable Personal Use Policy Page 11
- Data Handling Security Policy Page 13
- Security Incidents Policy Page 17
- Records Management Policy Page 20
Data Protection Policy

General rules in complying with Data Protection law

What must I do?

- **MUST**: All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals.
- **MUST**: Where personal data is used we must make sure that the data subjects have access to a complete and current **Privacy Notice**.
- **MUST**: We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which involves the use of personal data.
- **MUST**: We must process only the **minimum** amount of personal data necessary to deliver services.
- **MUST**: All employees who record opinions or intentions about service users must do so carefully and professionally.
- **MUST**: We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition.
- **MUST**: Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
- **MUST**: Consent will **expire** at the end of each 'Key Stage' period unless it is reconfirmed.
- **MUST**: We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
- **MUST**: If we receive a request from a member of the public or colleagues asking to access their personal data, we must handle it as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the **Education (Pupil Information) (England) Regulations 2005**.
- **MUST**: If we receive a request from anyone asking to access the personal data of someone other than themselves, we must fully consider Data Protection law before disclosing it.
- **MUST**: When someone contacts us requesting we change the way we are processing their personal data, we must consider their rights under Data Protection law.
- **MUST NOT**: You must not access personal data which you have **no right to view**.
- **MUST**: You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so.
- **MUST**: You must **share** personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer or SIRO.
- **MUST**: Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this must be done in compliance with the law and the regulator's Code of Practice.
- **MUST**: All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.
Heathlands Primary School GDPR Policies

- **MUST**: When using ‘data matching’ techniques, this must only be done for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate.
- **MUST**: We must maintain an up to date entry in the Public Register of Data Controllers
- **MUST**: Where personal data needs to be anonymised or pseudonymised, for example for research purposes, we must follow the relevant procedure
- **MUST NOT**: You must not share any personal data held by us with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or Data Protection Officer
- **MUST**: We must identify Special Categories of personal data and make sure it is handled with appropriate security and only accessible to authorised persons
- **MUST**: When sending Special Category data to an external person or organisation, it should be marked as “OFFICIAL-SENSITIVE” and where possible, sent by a secure method

**Why must I do it?**

- To comply with legislation
- To comply with Data Protection legislation which requires us to make the data subject aware of how we will handle their personal data
- To ensure that the rights of the Data Subject are protected in any proposed new activity or change to an existing one
- The law states that we must only process the minimum amount of information needed to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
- To maintain professional standards and to assist in defending the validity of such comments if the data subject exercises their rights to ask us to amend or delete their personal data if they feel it to be inaccurate.
- To comply with a principle of Data Protection law
- To comply with Data Protection law. Where processing does not rely on a legal condition other than consent
- When using personal data for marketing and promoting services it is unlikely that any lawful condition other than consent would apply.
- Consent can only be valid for a reasonable period of time.
- To comply with a principle of Data Protection law.
- To comply with the right to access personal data
- To comply with a principle of Data Protection law.
- To comply with the rights of the Data Subject under Data Protection law
- Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
- Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
- To comply with the legal requirements to keep personal secure but also to ensure that where there are legal grounds to share information in a managed way that this is done correctly.
- The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances recordings may be accessed e.g. to investigate alleged criminal activity or breaches of Organisation policy etc.
- To comply with a principle in Data Protection law and the Data Protection Officer governance requirements
- To comply with the Data Subject’s rights
- This is a regulatory requirement and allows the public to see what personal information we hold to support transparency
- Where personal data is used for research purposes, the processing of the data can be legitimised by provisions within Data Protection law
- To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would here. Personal data transferred overseas (including hosted solutions) must be securely handled under the same or substantially similar provisions that exist under the Data Protection Act.
- To comply with Article 9 of GDPR
- To comply with Article 9 of GDPR and comply with a principle of Data Protection law requiring personal data is processed with appropriate security measures

How must I do it?

- By following the points in this policy
- By approving and reviewing a compliant privacy notice in line with the Privacy Notice Procedure and making it available to the data subjects
- By completing and approving a Privacy Impact Assessment, or Data Protection Impact Assessment where the processing is ‘high risk’ to the rights of the data subjects.
- By ensuring that the means we use to gather personal data (such as forms etc.) only ask for the information that is required in order to deliver the service.
- By considering that anything committed to record about an individual may be accessible by that individual in the future or challenged over its accuracy.
- For example, there should be at least an annual check of the currency of data held about service users and whenever contact is re-established with a service user, you should check that the information you hold about them is still correct.
- By following the points in the Consent Procedure
- By following the points in the Consent Procedure
Heathlands Primary School GDPR Policies

- By following the points in the Consent Procedure. Parents/Guardians of pupils in the last year of a key stage should expect a communication to ask them to refresh their consents. If they do not respond ahead of a deadline date then consent should be assumed to be no longer valid.
- By following the points in the Records Management Policy. We must review personal data regularly and delete information which is no longer required; although we must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows us to keep indefinitely personal data processed only for historical, statistical or research purposes. The Retention Schedule will give guidance in these areas.
- By following the points in the Statutory Requests for Information Policy. We must be aware that data subjects can ask others to make a request on their behalf. There must be evidence of consent provided by the Data Subject to support this.
- By following the points in the Statutory Requests for Information Policy. Such requests would typically be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Justice law if for a criminal investigation, however the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law.
- By reviewing the impact of any requested change on any statutory duty being fulfilled by the Organisation.
- By being aware through training and guidance from your manager on what information is appropriate for you to access to do your job. Systems and other data storage must be designed to protect access to personal data. You must inform your manager if you have access to data which you suspect you are not entitled to view.
- By ensuring appropriate security controls are in place and rules to support those controls are followed. The following should be in place:
  - technical methods, such as encryption, password protection of systems, restricting access to network folders;
  - physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
  - organisational measures, such as:
    - Providing appropriate induction and training so that staff know what is expected of them
    - Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
      - Making sure that passwords are kept secure, forced to be changed after an agreed period and are never shared
- Consult your manager, any procedure guidance or any library of sharing agreements managed by the Organisation. Consult the Data Protection Officer or SIRO in one-off cases of sharing.
- By ensuring that employees and members of the public are fully aware of what personal data is being recorded about them and why, and it what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant codes of practice captured in the Surveillance Management Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016)
By completing compulsory training courses relevant to your role. Records will be kept of induction training and annual refresher training. Training content for each role will be determined by feedback on current training methods and the outcome of investigating security incidents. This will be reviewed frequently.

By ensuring an Impact Assessment has been approved for the activity

The entry should be reviewed annually and an update is to be made when any change to the purposes of processing personal data occur

Follow the guidance in the Data Minimisation Procedure

Consult the Data Protection Officer over any proposed sharing outside of the UK. If you are a manager who is proposing a change to or implementing a new system which may involve the hosting of personal data in a nation outside the UK, this must be first assessed by a Privacy Impact Assessment, which must be approved by your SIRO and Data Protection Officer

Special Categories of Personal Data are information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation. Where this data is held it should be stored securely and in a way that access is restricted only to those internal staff that have a valid need to access it. It should only be shared externally after verifying that the recipient is entitled to access this data and through secure means.

Hard-copy packages must be marked as such by writing on the exterior of the package. Emails should contain the wording in the 'subject' field before the email title. Refer to the Records of Processing Activity document and the register of Data Flows for clear instruction on how you are expected to handle sending the data securely according to the particular activity you are undertaking.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 (including the General Data Protection Regulation 2016
- Article 8, The Human Rights Act 1998
- Education (Pupil Information) (England) Regulations 2005

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.
Statutory Requests for Information Policy

Requirements for managing requests for information to comply with the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations (EIR), the General Data Protection Regulations 2016 and the Data Protection Act 2018.

What must I do?

For all types of request for Information:

- **MUST:** We must **correctly identify** the law which applies to the information being requested and manage the request in compliance with that law.
- **MUST:** Information should be **released** unless there a strong legal justification for withholding it.
- **MUST:** Whenever we **refuse** to provide information, we must clearly and fully explain the reasons why.
- **MUST:** We must provide **advice and assistance** to people making a request.
- **MUST:** We must always try to **reply** as quickly as possible, but always within the legal deadline.
- **MUST:** All employees must promptly **provide** all relevant information to a request co-ordinator if asked for it.
- **MUST:** If we decide to **charge** for information, we must do so in accordance with a published policy.
- **MUST:** Where reasonable and practical, we must provide the information in the **format** requested by the applicant.
- **MUST:** When we respond to a request, we must tell the requestor about our **internal review** process.
- **MUST:** When responding to a complaint, we must advise the requestor that they may **complain to the ICO** if they remain unhappy with the outcome.
- **MUST:** We must maintain an up to date Publication Scheme available on our website to meet our obligations under FOI/EIR.

Why must I do it?

- The requestor does not have to specify under what legislation they are making a request. It is our responsibility to correctly identify which legislation applies.
- We serve the public. We should not hide information from them. The Acts are intended to make us more accountable to the public, to make our processes more transparent, and to encourage the public to trust us. Information should be released unless we can strongly justify withholding it (embarrassment is not a sufficient reason to withhold information). In some cases, we may have to release non-personal information because it is in the public interest although it might otherwise have been considered exempt. Also, it is a legal offence to deliberately withhold or destroy requested information where there is no legal reason to do so.
- We will not be obliged to provide all or part of the information requested if a legal justification applies. If we believe a reason does apply then we must help the public to challenge our decisions effectively by giving our reasons and doing so clearly and fully in line with the requirements of the Acts. This is a legal requirement.
- The Acts require us to assist requestors, especially where we may be considering refusing a request, in guiding the public on how to clarify or re-scope their request to achieve the best outcome. This is a legal requirement.
Heathlands Primary School GDPR Policies

- The laws provide statutory deadlines for responding to a request; FOI & EIR – 20 working days and DPA one month. There are limited reasons to extend the deadlines. The laws expect information to be well managed and accessible, therefore there is an assumption that requests should be routinely responded to well in advance of the deadline.
- In order to comply with regulator and corporate targets for fulfilling requests, all employees have a role to play in making information relevant to the request available promptly so that a response can be drafted within the timescale.
- The laws require us to make clear the basis for charging to ensure that charges are fair and un-obstructive. We must tell requestors whether a charge applies before we provide the information and we should tell them what that charge will be.
- The acts duty on us to provide information in a format that the requester would find most convenient to their needs. We may refuse unreasonable demands and charge in certain cases, but in principle the requestor should be able to receive the information in the way they specify.
- It is a requirement of the act to have an internal review process. Where a requestor expresses dissatisfaction with a response, this must be treated as a complaint. The act states that expressing dissatisfaction is enough to require us to treat it as such. The ICO requires us to complete the internal review process before it will accept an escalation of a complaint to their office.
- This is a statutory requirement.
- This is a statutory requirement.

**How must I do it?**

- Follow guidance and training to correctly identify whether the request should be handled under FOI, EIR or DPA/GDPR.
- By following the points of this policy and accompanying guidance and training
- Ensure the employee making decisions about what can be released and drafting the response has access to legal guidance in order to make the response full and compliant with the law.
- Discuss the likely response with the requestor if their request is likely to be refused and explain options that would help them receive as useful a response as possible within the limits of the law. Although we should not ask requestors what they intend to do with the information they have requested, we can explain what we do hold and what is likely to be disclosable to them.
- We must record performance against the statutory deadlines to ensure we are aware of how well we are complying with the law and to help make changes to processes if necessary.
- Make sure the information you manage is accessible and well structured so that you can retrieve it quickly when requested.
- It is not lawful to charge for information without a published policy explaining the basis for arriving at a fee. In the absence of a published policy, charges are not made.
- There must be strong prohibitive reasons not to provide information in a format that is within our ability to provide. Conversion to a new format is however different to having to significantly edit and rearrange information to make it legible in the format requested. Under the latter circumstances, a refusal may be valid but advice should be sought if unsure.
- We choose to manage complaints (known as Internal Reviews) within 20 working days. Where a simple error has been made in the response it may be that the issue can be resolved informally. If not, then a full review of how the request was handled is required. This
must be undertaken by an employee who was not involved in drafting or approving the original request, although the employee drafting the response may discuss how the original request was handled with those involved.

- Ensure that the contact details for the ICO are provided to the requestor on any response documentation and explain when it is appropriate to escalate a complaint the ICO in order to make requestors aware of their rights.
- To enable requestors to understand the types of information the organisation holds, what format it can be disclosed in, and whether charges apply.

**What if I need to do something against the policy?**

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

**References**

- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulation 2005
- Education (Pupil Information) (England) Regulations 2005

**Breach Statement**

Breach of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.
Acceptable Personal Use of Resources and Assets Policy

Explaining what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use

What must I do?

- **MUST**: You must use our facilities **economically**; your personal use must not create extra costs for us
- **MUST NOT**: You must not use our facilities to undertake any unlawful, libellous, immoral or offensive **activities**, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material
- **MUST NOT**: Personal use must not interfere with your **productivity** and how you carry out your duties
- **MUST NOT**: Personal use must not reflect adversely on our **reputation**
- **MUST NOT**: You must not leave **personal-use websites** open during your working time, even if they are minimised on your screen and you are not actively viewing/using them
- **MUST NOT**: You must not use browsers or access/attempt to access sites that are knowingly **unacceptable**, even if this is in your own time
- **MUST NOT**: You must not send or forward chain, joke or spam emails
- **MUST NOT**: You must not use the Organisation’s facilities for **commercial purposes** not approved by us or for personal financial gain
- **MUST NOT**: You must not use your access rights or identity as an employee to **mislead** another person, for personal gain or in any other way which is inconsistent with your role
- **MUST NOT**: You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
- **MUST NOT**: When you print, photocopy, scan or fax official-sensitive information, you must not leave the information **unattended**.
- **MUST NOT**: You must not **connect** any equipment to our IT network that has not been approved
- **MUST NOT**: You must not do anything that would **compromise** the security of the information held by us, such as downloading/spreading any harmful virus/program or disabling or changing standard security settings
- **MUST NOT**: You must not make personal use of the information available to you that is not available to the **public**

Why must I do it?

- **ALL**: To ensure we use our IT and other facilities resources effectively, making sure that our reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes
How must I do it?

- By checking with your manager or where you have any uncertainty over what is appropriate
- By complying with the points of this policy
- You must only make personal use of our IT facilities outside of time you are recording or is designated as your ‘working hours’
- By complying with the points of this policy
- Closing websites when you are not actively using them
- By taking care over the sites you are about to open, including reading search report information before opening
- By deleting such items if you receive them.
- By checking with your manager where you have any uncertainty over what is appropriate
- By checking with your manager where you have any uncertainty over what is appropriate
- If you are not sure if you are authorised to disclose information, speak with your manager in the first instance
- If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.
- Check that equipment has been tagged or marked as an accepted and managed device before insertion/connection.
- IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
- If you wish to utilise Organisation data in a personal capacity, you must make a formal request for information to the Organisation.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018
- General Data Protection Regulations 2016

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.
Data Handling Security Policy

Responsibilities for managing IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations

What must I do?

- **MUST**: You must take **responsibility** for the security of the equipment allocated to you and that is in your custody.
- **MUST**: When you are physically **transporting** our data outside of our premises, on any medium, you must take steps to keep it secure.
- **MUST**: You must not leave Official-Sensitive data unattended in a **vehicle** for longer than 10 minutes, and always keep it out of sight.
- **MUST**: You must take appropriate steps to secure our data at **home** and other organisations' **premises**.
- **MUST**: If working with our data on approved unmanaged equipment, you must **remove** the data when finished.
- **MUST**: If you are taking Official-Sensitive information out of the office, this must be **recorded**.
- **MUST**: You must make sure that conversations discussing sensitive data are only audible by an **appropriate audience**.
- **MUST NOT**: You must not allow anyone **access** to your IT equipment through your IT account.
- **MUST NOT**: You must not use any equipment to store our business data that has not been **approved**.
- **MUST NOT**: You must not allow unauthorised people to be able view information on your IT equipment **display**.
- **MUST NOT**: You must not save your passwords to any web based system which holds our data in the browser.
- **MUST**: You must always use an approved secure method of **disposing** of physical documents and data storage devices.
- **MUST**: You must **return** all equipment which has been issued to you by us prior to leaving your employment.
- **MUST**: You must **report** as quickly as possible if your equipment is lost or stolen and assist with any **investigation**.
- **MUST**: You must ensure that all security functions are **enabled** on your portable equipment, such as pin codes and password access.
- **MUST**: You must keep your portable equipment, **clean and serviceable**, including keeping it charged.
- **MUST NOT**: You must not take any of our equipment **abroad** unless you are traveling in a business capacity with approval.
- **MUST NOT**: You must not give your portable equipment to **another person** if you are not using it.
- **MUST**: You must immediately raise as a security incident any loss, unlawful access or theft of the data we are responsible for.

Why must I do it?

- You are the custodian of the equipment; it is your responsibility to keep it physically secure.
- To prevent any accidental loss (for example papers or removable media accidentally falling out of bags), or theft (by exposing papers or equipment by not securing them properly). Although laptops are encrypted, it is still possible for a motivated criminal with technical knowledge to access data.
Experience in investigation of thefts at employee homes has shown that if equipment is left in plain view it will be taken, whereas storing away out of sight when not in use results in fewer cases of theft.

To prevent accidental loss, unauthorised use and theft in your home and whilst in other Organisations' premises.

Data in the browser cache or temporary file storage may be useable by other subsequent users of the same device.

To make sure that others know who has custody of important information at all times.

We have a duty even within our premises to make sure that personal data is only made available to those with the business need to access it. This applies verbally as well as in recorded form.

All activity on your IT account is assumed to be yours. Logs of activity are maintained. You are accountable for any wrongdoing through your account.

Equipment purchased through us will have appropriate technical security installed, or will have best practice guidance on how to use the equipment securely.

Unauthorised people may be able to see sensitive information on your screen.

This introduces the risk of someone who can gain access to your device also getting easy access to the data on your work emails.

Secure destruction processes safeguard the information stored on IT devices and physical documents and prevent data being accessed by unauthorised persons.

Providing such items is costly and represents a data security risk. We reserve the right to treat instances of refusing to return such items as theft.

This enables to promptly remove data from devices remotely, therefore reducing the risk. Such investigations may lead to disciplinary action, and in extreme circumstances could lead to the service area seeking financial remuneration. Having all the information about a security incident helps us to resolve it quickly and take the appropriate action to manage any risks of information being lost.

Such measures help keep the device and information available on it secure.

Correct use and basic maintenance helps us gain best value from the investment we make in our equipment.

We need to be aware of any risk of using our equipment abroad, especially in countries who do not share common legislation to safeguard personal data, and where internet services may expose our devices and therefore our network to malicious threats. There may also be costs involved in replacing equipment which is subject to precautionary measures on your return. The costs of reviewing requests and replacing equipment are not appropriate for instances of employees wanting to use equipment whilst on holiday. Business continuity cover arrangements and delegation should be able to manage instances of leave.

Portable equipment is asset managed across our estate and assigned to an individual. Being able to accurately evidence who holds what equipment is an important assurance we give to the Information Commissioner's Office over our ability to manage our assets and the information available on them.

Reporting security incidents allows us to manage our risks and ensure that we take step to avoid similar occurrences.
How must I do it?

- By following the points in this policy
- This relates to paper files, phones, laptops and other removable media such as USB memory sticks, discs and external hard drives. Use equipment which reduces physical effort in order to appropriately manage the risk of overloading or forcing a tenuous hold over physical documents which can result in accidental loss of control over the information. Items should not be visible to others; even partially. This means they should be secured within an appropriate bag or other robust container. Laptop bags are suitable, ensuring that zip compartments are closed concealing the contents. Employees frequently needing to transport quantities of information that are too bulky to carry under full control and/or transporting Official-Sensitive data must review with their manager the need for being supplied with wheeled suitcase-style equipment with code locks to further secure the information.
- Items such as paper files, phones, laptops and other removable media left in a vehicle should only be unattended for a short period of time (maximum of 10 minutes for Official-Sensitive information) and must be kept out of sight (not visible to anyone looking in through a vehicle window). Locked in a boot is considered secure for a limited time if it cannot be taken with you when leaving a car.
- Only authorised users (this means people with IT accounts provided by us) can use your IT equipment and only through using their own accounts. It is not acceptable to allow family members or friends to use IT facilities or have access to our information even if you are present. You must also make sure that when IT equipment and hard-copy information is not in use that it is stored securely out of sight.
- If you are located temporarily in the premises of another organisation or your work requires site visits or entering homes of service users, you must secure IT equipment and hard-copy information. Make sure you understand what information your role allows you to share with partners or service users and limit the information you make available accordingly. Your role may require you to allow someone to have access to your IT device, for example a service user in their home may need to read content on your screen and select options from menus. You must understand the limits of their access requirements and manage this access. If you are located in the premises of another Organisation as a semi-permanent base, it is reasonable to leave our data in your allocated office or team area provided that you have the same level of secure storage for equipment and hard-copy as you would in our buildings. You must get approval for storing our data in premises not managed by us from your manager if the location is anything other than your permanent office base.
- On most systems this can be done by selecting ‘public network’ when setting up the access. Otherwise it will need to be done manually in the web browser options.
- You should have access to systems or a log which allow you to ‘sign-out’ or record what information you are taking custody of, when taken, when returned and (if appropriate) why and under whose authority. Where such facilities are available they must be used.
- Most employees who handle Official-Sensitive data will have been located with those of similar roles or be in self-contained spaces. However, there is always the possibility of unauthorised persons being in the vicinity when you may need to discuss sensitive personal data with colleagues near you or over the phone, or display on a screen. You must make sure as the person who is custodian of the information that it is appropriate to discuss or display the information in the circumstances. You must make sure that if you are overhearing or otherwise being exposed to data to which you should not have access, you alert the information custodian to the fact that they are not managing the information appropriately.
- Make sure that you lock your screen at all times if you leave your laptop/ desktop or phone unattended to avoid someone accessing your account without your knowledge. Always supervise and monitor anyone using your device in the strictly limited circumstances where allowing someone access is acceptable (for example a service user in their home may need to read content on your screen and select options from menus).
This is including but not limited to computers, printers, phones, tablets and cameras. Order equipment through us and follow any conditions of use associated with an exception to policy, and follow any standard instructions that are supplied with the device. Where technically feasible, encryption will be applied to secure the contents of storage devices.

Ensure that no-one in your vicinity can see and read the screen of your device. This applies to working in public places (such as cafes with Wi-Fi), in partner organisations’ offices, and even when hotdesking within our premises when viewing Official-Sensitive data unless you are certain that others around you are allowed to see similar data.

Do not approve any offer from your device’s browser to save your password when logging in to OWA.

Make use of the facilities for secure disposal of paper documents and IT storage devices.

Follow a leavers checklist with your manager

Raise a security incident and inform your manager. Provide any information requested of you by an investigating officer

Follow the instructions provided to you with your equipment

Ensure that any equipment given or received by you is through our processes

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Article 8, The Human Rights Act 1998

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.
Security Incidents Policy

A security incident is a confirmed breach, potential breach or 'near-miss' breach of one of the school’s information policies

What must I do?

- **MUST**: If you discover a security incident, you must immediately **report** it
- **MUST**: When reporting the incident, you must **provide** as much information as possible
- **MUST**: The Investigating Officer must **complete** investigations and complete an outcome report (see Procedures for Reporting or Handling a Security Incident)
- **MUST**: All staff must support investigations into incidents as required
- **MUST**: Maintain a full **record** of each incident from reporting to closure
- **MUST**: The Headteacher/SIRO must support the investigation of **major and critical** incidents
- **MUST**: Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident
- **MUST**: Major and critical incidents must be referred to the Data Protection Officer.

Why must I do it?

- Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective
- To help us quickly assess the severity of the incident and to speed up the investigation
- Carry out an effective process appropriate to the severity of the incident
- Ensure the process is followed to completion
- Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents
- Ensure that all incidents are handled in a timely manner
- Ensure that serious incidents are reviewed against the criteria for reporting to the regulator.

How must I do it?

- Please notify the school office. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible.
- Include full details of the incident such as dates, names and any remedial action that has been taken.
- Where appropriate, undertake the following:
  a. Identify expected outcomes, stakeholders and any policies breached.
  b. Speak to staff involved.
  c. Record evidence and keep an audit trail of events and evidence supporting decisions taken
  d. Get expert help
  e. Escalate
  f. Inform data subjects (service users, staff) where appropriate
  g. Identify and manage risks of the incident
  h. Commence disciplinary action, or record why not
  i. Develop and implement a communications plan where appropriate
  j. Put in place controls to prevent recurrence
  k. Complete the Incident Outcome Report
- Where appropriate, undertake the following:
  a. Work with the SIRO to investigate major security incidents.
  b. Assess the outcome to ensure the appropriate action has been taken.
  c. Provide knowledge and advice, and carry out any recommended actions for major or critical incidents, where required.
- Undertake the following:
  a. Classify the Security Incident
  b. Verify the details and oversee the investigation
  c. Work with SIRO to investigate major security incidents.
  d. Advise, support and intervene as appropriate
  e. Review Incident Outcome Reports and close
- For major and critical incidents:
  a. Undertake the investigation (critical only)
  b. Work with SIRO (major only)
  c. Assess if it is necessary for the security incident to be reported to the ICO.
  d. Complete an outcome report and recommend remedial actions.
- Follow the process outlined in the school’s Procedures for Reporting or Handling a Security Incident

**What if I need to do something against the policy?**

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.
References

- Data Protection Act 2018

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.
Records Management Policy

Responsibilities for management of information to support secure access and effective retention, destruction and preservation processes

What must I do?

- **MUST**: You must **document** your work activities in line with procedures
- **MUST**: You must store all work information in the format and **medium** best suited to its use in line with procedures
- **MUST**: You must ensure that the information you manage is only known to an **appropriate audience**
- **MUST**: All information in any format which we hold as a record of our activity must be **retained** after ‘closure’ in line with **Retention Guidelines**
- **MUST**: Owners must regularly **review** information in line with **Retention Guidelines** to make best use of the available storage space
- **MUST**: We must **monitor** the success of the review process to maintain compliance with the law
- **MUST**: You must manage Pupil records in line with **best practice** and specific system **guidance**
- **MUST**: You must follow **Good Practice for Managing E-Mail** when storing **emails** as records
- **MUST**: We must ensure that the **facilities** available for storing and managing information meet legal requirements and **best practice**
- **MUST**: We must maintain a **selection procedure** for identifying, reviewing and managing records with **historical value**
- **MUST NOT**: You must not store business information on a personal drive or on equipment not provided by the Organisation
- **MUST**: All Information **Assets** identified on the Register must be associated with a retention period from the **Retention Guidelines**.
- **MUST**: The **Retention Guidelines** must be reviewed for **changes** in legislation and the Organisation’s business needs.
- **MUST**: When archiving paper records, information on ownership, retention and indexing quality must be recorded.
- **MUST NOT**: You must not use the archive storage services of any other commercial company than the **approved supplier**
- **MUST**: You must ensure that personal information processes are recorded in your Records of Processing Activity

Why must I do it?

- These measures ensure Organisation information, where appropriate to do so, is shared effectively to support efficient business processes and maintain effective service delivery to customers.
- Managing records in line with the best practice guidance fulfils duties under the section 46 Code of Practice on Records Management under the Freedom of Information Act 2000. Retention Guidelines are published so there is clear communication to customers over what information should still be available to them if they wish to make a request. To retain information too long or to destroy too soon leaves us open to criticisms on openness and transparency, and in some cases, compliance with the law.
- In order to comply with the Section 46 Code of Practice (see above) we must ensure that we are destroying all related information across all formats. For example, destroying a paper file on a project but keeping all the electronic documents about the project in a shared network folder can cause problems if a Freedom of Information request is received. The request co-ordinator assumes that as the paper file is destroyed then we do not hold any information and responds accordingly. We would then be in breach of the act.
- Records of Processing Activity are a legal requirement under the General Data Protection Act 2016 as applied by the Data Protection Act 2018.

### How must I do it?

- Employees are aware of [best practice](#) requirements and any guidance on use of specific systems through training and communications.
- You must ensure that paper files are accessible to authorised colleagues in your absence, by ensuring others know where to find keys to lockable storage areas. You must be aware of who information should be shared with, and ensure it is only shared with that audience.
- You must ensure that you save electronic information in a shared environment, but with appropriate access controls if the information has a restricted audience.
- Follow the [best practice](#) guidance and any superseding amendments made by the Organisation.
- Designated employees must gather performance data on activities within the scope of this policy for review by the Data Protection Officer and the Leadership Team.
- Follow the [best practice](#) guidance and any superseding amendments made by the Organisation.
- The organisation must approve and regular review facilities such as systems and physical storage as appropriate against security requirements in Data Protection Law, and all employees must help maintain security standards by following procedure.
- Records can be identified for preservation at any point in the records lifecycle, but will not transfer until we have no ongoing administrative need (i.e. at the end of a retention period). When information is due to be destroyed, there should be a final review to select records for transfer to the Nottinghamshire Record Office.
- By only storing all business information on the relevant systems designated by the Organisation and by using only equipment approved by the Organisation.
- The Information Asset Owner is responsible for ensuring that Information Asset Managers amend entries on the Information Asset Register to show the correct retention period from the schedule.
- A policy review (at least annually) must review the provisions of [best practice](#) retention guidance and make any necessary amendments, documenting the reasons for change and managing affected records accordingly.
- We must complete and retain archiving indexes providing the relevant information about paper records in storage, ensuring that the Organisation is aware of what information it holds at all times and when they can be reviewed.
- Any use of a commercial storage provider must be assessed and approved to ensure the right security and financial provisions are place. Use of alternatives that have not been approved may not provide value for money and may not provide secure services.
- Records of Processing Activity must be maintained and regularly reviewed to meet your legal obligations.
What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Article 8, The Human Rights Act 1998
- Code of Practice on Records Management (under Section 46 of the FoIA)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.