The School's Access to Information: Rule book and policies

For School Staff

ISO27001:2005
Information Security Management System

Version 1 – September 2019
Owner: School's Data Protection Team
Review Date: September 2020
Approved by: Information Governance Group

Version control table

Version Number	Date	Purpose/Change	Reviewer / Authoriser
1.0	01/09/2019	Council's Access To Informaiton: Rulebook and policies adapted for school use.	School's Data Protection Team

Contents

About this document

The Access to Information rules are mandatory reading for all school staff (including agency and voluntary staff), Contractors, and organisations who work with our systems and information to provide services. They set out the school rules on:

- Working with information – electronic, paper, microfiche, CD – any format – and however that work is performed.
- Using the everyday electronics and technologies that support each of us in doing our work.

We have written it as a set of 'rule books', to make it easier to read and understand.

About the 'Rules'

The 'rules' set out the **Do's** and **Don'ts** of working with the Information and related systems of the school.

Everyone listed above **MUST:**

- Ensure they have **read and understood** the rules, and know how they apply to them. Ask your line manager or School's Data Protection Team if you are uncertain.
- **Act in 'good faith'** – and not breach the rules. While exceptions can be given, they must be given formally, by the School's Data Protection Team.
- **Report** any incidents where the rules have been broken **– or where they think that it is likely that they will be.**

School Business Managers

1. **MUST** ensure that members of their team are aware of the rules, and have been **trained** on them.
2. **MAY** choose to have further, more restrictive rules in their areas. Local management takes responsibility for such rules and their implementation, and assuring that they are in line with other school policies and standards. Advice should be sought from HR.

Breaking the 'Rules'

- If rules are deliberately broken or ignored, the school reserves the right to investigate and take appropriate action. Further details are available in the supplements.

Staff: Quick Index

All the rules in the rule books apply to school staff – but it can be helpful to look at some sections first. Here is a quick 'map' of some of the key documents to help you.

Everyone Handles Information when they work

- Rule Book 1: Managing Information
- Rule Book 3: Public access to information
- Rule Book 4: Physical Security
- Rule Book 14: Reporting incidents

Do you Share information with others?

- Rule Book 2: Sharing Information

Do you Use school computers or technology?

- Rule Book 6: Using school computers, software and 'apps'
- Rule Book 7: Keeping our systems secure
- Rule Book 12: Sending Messages
- Rule Book 13: Using School Telephones, Mobiles & Voicemail

Do you Work flexibly in or out of the office?

- Rule Book 8: Working out of the school
- Rule Book 9: 'Bring your own device'

Do you Browse the internet?

- Rule Book 10: The internet
- Rule Book 11: Social Media
- Rule Book 15: Cloud Services

Rule Book Detailed Index

The remainder of this document is divided into a series of 'Rule Books' or sections which can be read individually.

All sections apply to **YOU**, except the 'Specific Policies' which apply to the users of those services, or if a written exemption has been granted.

Rule number	Title
	Telephones
13	Using school telephones, mobiles and voicemail
	Incidents
14	Reporting Incidents and 'near-misses' – your responsibilities
	Specific Policies
15	Cloud Services – School Approved, Go4Schools, OneDrive, Google Drive, etc..
	Supplements
A	How the school applies the rules, and how you can obtain an exemption
B	How the school monitors use of information services, and how it affects you

Access to Information: Rule 1

1 Managing Information

1.1 Background

- Managing Information correctly is part of offering a good service.
- Pupils, parents and staff can get hurt, and the school's reputation damaged, if the **confidentiality** of information is broken. Information **must** only be accessed by people who are authorised to view it to prevent data breaches.
- **Inaccurate** information is of no use to the school. It makes staff work inefficiently, causes confusion and wrong decision making.
- If information is not **easily available** when needed, services are not able to be delivered, which could lead to massive implications.

1.1.1 Important to know

- Anyone may request access to information held by the school, with a few exemptions, so data **quality** must be ensured to avoid errors and people losing trust in the school.
- It is **against** the Data Protection Act (2018) for the school to retain certain kinds of information for longer than necessary.
- As a school, there is a legal requirement to hold certain types of information for a minimum amount of time. This is known as a retention period.

1.1.2 Headteacher's / GDPR Lead's responsibilities

- **You MUST**:
    - Understand what information you are responsible for – are you the *'information asset owner'* or *'responsible manager"*?
    - Assess the risks to that information.
    - Take appropriate action to ensure it is managed and protected appropriately.
    - Train your team(s) on their responsibilities.

1.1.3 Everyone's responsibilities

Everyone **MUST**:

- Work with information as per the rules, guidance, procedures and policies given to them.
- Understand that there is a duty of confidentiality which means that any personal information or data that is accessed must be safeguarded.

1.2 Creating information

Everyone *creates* information as part of their work – either by writing new records – e.g. about a parent and or pupil, or when they *interpret* other information as part of a school.

Everyone MUST:

- Ensure they create information that is:
    - **Clear, Accurate & Factual** – so that it cannot be misunderstood or challenged
    - **Relevant & not excessive** – i.e. in line with school requirements
- Ensure information is stored correctly – in the right way, right place
    - Documents must be **titled appropriately** when stored on a computer system. – *"the filename 'new.doc' means nothing!"*
    - Information must be **stored electronically** where possible, in the correct and agreed location
      – i.e. if SIMS' is where pupil data records are stored, they should be

stored in the correct format, and not on a paper file or in a 'home area' on the network.

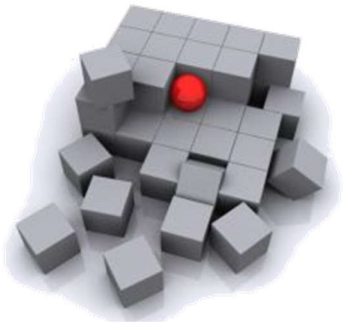
You **MUST NOT:**

- Document opinion or assumptions – unless it is required to do so within a job description.
- Document the views of others, or 'hearsay', without the consent of the other people, unless it is part of the job.
- Use language which may be insulting, easily misinterpreted, or does not consider the Equality and Diversity policies of the school.

Be AWARE that:

- Any record could be requested by a member of staff, pupil or parent at any time. While there are *processes* to make sure this is done correctly, there are a few exemptions to what can be handed out. Please contact the School's Data Protection Officer before applying any exemption.

1.3 Storing & retaining information



1.1.2 Headteacher's / GDPR Lead's responsibilities:

You MUST:

- Ensure that information remains easy to access throughout its life, considering its purpose and the law.
  Certain records must be stored for a minimum amount of time; certain records for a maximum. This is known as the record retention period.
- Ensure that the storage location manages the **risks** to that information and supports its *security (confidentiality), whether it may be subject to damage over time (integrity), or the need for it to be available (accessibility, or e.g. protected against fire/theft).*
- *Ensure people are aware of how long information needs to be kept for – and that processes are documented and followed. Staff should know how to check and understand how to apply the school's record retention schedules.*

Everyone **MUST**

- Ensure that temporary paper copies of information are disposed of appropriately (securely if they contain sensitive information) unless there is an agreed school need to keep them.

1.4 Disposing of Information

Before disposing of information, everyone **MUST:**

- Check whether local procedures or the law allow or require that information to be destroyed.
- Consider the **value** of that record to the school if it was retained, versus the **cost** of retaining it – and ask appropriate questions if there is a concern.
- Follow or create procedures that decide whether to record, how and when information has been destroyed
  e.g. this applies if bulk files were to be disposed of, and should this be recorded. Some types of record may need to be 'tracked' throughout their lives.

To dispose of information:

- A secure method of disposal **MUST** be used:
  - For paper information and CDs, cross-cut shredding can be used.
  - If an external disposal company is used, a certificate of disposal **MUST** be obtained.

Be AWARE that:

- It is a criminal offence to destroy records when a request for disclosure has been received by the school, for example under Freedom of Information (FoI), the Data Protection legislation, the General Data Protection Regulations (GDPR) or the Environmental Information Regulations (EIR). Do not dispose of information on the basis that it might cause embarrassment to the school.

1.5 Transporting Information

- Other rules give guidance on Secure e-mail, which can be used to securely transport both small and large quantities of information to recipients.
- When transporting information, electronically or otherwise, it must be kept safe and secure. Everyone is responsible for making sure that information is transported securely, and individuals are **accountable** for their actions.

You MUST NOT:

- Take or send sensitive data, including individuals' personal details out of the school buildings in any format (paper, memory sticks, laptops, DVDs, phones etc), unless it is in a secured method agreed by the school's policy. *For paper information, this may be as simple as a locked briefcase or bag. For electronic information, encryption is required. Talk to the school's IT manager for more information.*
- Disclose information or data in your safekeeping to any party, unless it is part of your job, within your normal day-to-day working practices or in line with the school's 'whistleblowing' and or safeguarding procedures.
- Discuss or disclose information to any unauthorised third party – including staff that don't have the right to see it.

2 Sharing Information

Sharing information is part of providing excellent services. Information provided is shared with others in the school, the department of education, and others for legal or contractual requirements.

Everyone MUST:

- Make sure they are sharing:
  - **the right information**, with;
  - **the right people**, for;
  - **an agreed purpose**
- Follow procedures, agree on and take actions to reduce the risk of the information getting lost, or being passed to the wrong people.

Headteacher's / GDPR Lead's responsibilities:

You MUST:

- Ensure that relevant internal procedures and external agreements are in place to make sure information is shared in a responsible, safe way.
  - *The School's Data Protection Team can provide details of 'information sharing agreements' and 'Data Protection Impact Assessments (DPIAs)'. DPIAs and sharing agreements must be in place before sharing commences.*
  - *Contract terms must include clauses on safe information sharing and how information will be used.*

Everyone MUST:

- Mark sensitive information to show how sensitive it is – and help others understand what protection it needs.
- Check they are sharing the **minimum** information required.
  - Do not share information if it isn't relevant e.g. don't send an entire case file if only part of the information is needed.

  - For research and testing, information can be shared with less detail or can be anonymised.

- Make sure secure methods are used to share sensitive information.

You MUST NOT:

- Transmit sensitive or personal information if there is no authorisation to do so, or if it isn't protected against loss or unauthorised access.The school offers secure methods – like secure e-mail to help.

- Share information unless it's for a specific, agreed school purpose.

3 Public Access to Information: Data Protection & FOI

Staff members, parents and pupils have a **reasonable** right of access to information about themselves and the activities of the school, in fact, **any information that the school holds.**

There are some exemptions to this and the **School's Data Protection Team** have been trained in how to deal with these.

Everyone MUST:

- Be aware of their responsibilities under the Data Protection legislation, the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000 (FOI).
    - ***All** staff **must** complete the Introduction to GDPR for Schools Course.*
- Be aware of the **School's Data Protection Team's** procedures for dealing with requests for information.
- Familiarise themselves with who the GDPR lead is for their school and the contact information for the **School's Data Protection Team**.

You MUST NOT:

- Ignore a request for information.
- Disclose any **personal information without following information disclosure procedures**. Requests for personal information are covered by the Data Protection legislation/the GDPR and should be sent in writing to the **School's Data Protection Team (school.dpo@brent.gov.uk).**

Be AWARE that**:**

- If you receive a request for information, it must be sent to The School's Data Protection Team as quickly as possible, as there are legal time limits for the school to process and respond to such requests.
- It is an offence under FOIA and Data Protection legislation/GDPR to alter, deface, block, erase, destroy, or conceal information with the intention of preventing its disclosure, unless an appropriate exemption applies.

4 Physical Security

Everyone needs to play a part in physical security – to protect our information, people, buildings and equipment.

14.1 Basic Responsibilities

As a School business manager or GDPR Lead

You MUST

- Make sure that the information in your school is suitably protected, according to its sensitivity. Think about the impact on the school if it was released to an unauthorised party, became unfit for purpose, or unavailable. Consider fire, flood, theft or other risks.
- Consider the implications for school integrity.
- Brief staff about expectations and school policies regarding:
    - Clear desk policy;
    - Managing visitors and guests to your area;
    - Preventing unauthorised access to your area and its information;
    - What to do in the case of a security problem or incident;
    - Policies relating to fire safety and other health & safety issues.

Everyone MUST

- Make sure they are aware of school policies and guidance on:
    - Storage of information (including 'clear desk' policy);
    - Managing visitors;
    - Preventing unauthorised access to your school, work-area and the information within it;
    - Fire safety & Health & Safety.
- Report any incidents of theft, break-in, or any suspicious matters immediately to your line manager.

You MUST NOT

- Allow people who you don't know well, or who are not authorised, to enter the school office or areas where sensitive personal information is kept unless they can positively identify themselves.
    - It's **polite** to challenge people you don't know, rather than just letting them in.
    - It's **not polite** to put your colleagues, pupils and sensitive information at risk from strangers and intruders.
- Give or loan your school pass to anyone else, or give out door codes to unauthorised people. **Access will be logged as if it was you entering any secure area.**

5 Clear Desk and Paperless-First Policy

5.1 Background

It is best practice for the school to operate a clear desk policy

- for the benefit of colleagues.
- to maintain flexible working.
- to protect the security of information.

In support of the Green Agenda, efficiency and security, it is also best practice for the school to support a reduction in paper usage where it is reasonable and feasible to do so.

5.2 Clear Desk: Responsibilities

At the end of the day, you **must:**

- Put away all office papers or dispose of them securely as appropriate.
    - This includes files on the floor, surrounding area and left near printers
    - Papers should be stored in drawers or filing cabinets, and confidential or sensitive documents should be stored securely.
- Leave your desk in a reasonably clean and tidy state to reduce the probability of data breaches in cases of school burglary or any unauthorised access.

5.3 Paperless-first: Background

- Using paper to work with information:
    - Has an environmental impact and uses valuable resources.
    - Costs money: Paper, printer ink, printer maintenance.
    - Causes potential security issues – e.g. loss, which can result in the school being fined.
    - Means we need places to file and retrieve it – which costs more money and takes up valuable time.
- The school has limited storage available for paper.

- A single loss of information containing personal data could result in the school being fined up to 20 million Euros under current legislation.

5.4 Paperless-first: Responsibilities

- All staff and managers should consider whether using paper to deliver school business is in the interests of efficiency and security.
- Everyone should avoid unnecessary printing of information **"Think before you print"**.
- All staff MUST consider the risks of different ways of handling information, including paper and the opportunities available to minimise paper handling. If in doubt, they should consult the School's Data Protection Team for advice.
- School Business Managers MUST consider the full costs of paper-based solutions (including printing, archival, disposal) versus technology-based methods, and should seek the assistance of the school's IT Consultant in the consideration or development of alternate solutions.
- School Business Managers MUST review the costs of printing in their school area and consider whether efficiencies can be made.

6 Using school devices, software and 'apps'

Background

- This rule sets out what you **must** and **must not** do when using:
    - technical equipment that the school provides for staff – a PC, laptop, tablet, iPad, iPhone, etc. – and the software or 'apps' that run on it.
- These facilities are provided to help the school serve its duty – they need to be treated with responsibility and respect.

6.1 Basic Responsibilities

Everyone MUST:

- Treat any school provided technical equipment with a high level of care.
- Report any fault, damage or loss of equipment immediately to the school's IT Consultant.
- Store school documents and data on systems provided by or agreed by the school – e.g. your 'shared drive' etc.

You MUST NOT:

- Store sensitive or important school documents and data on systems **not** agreed by the school, for example on local hard drives ('Drive C:\') or at home where it can get lost or accessed easily.
- 'Plug in' any equipment to the school's network which is not managed by the school's IT Consultant, **unless** the school has agreed on this. e.g. removal devices (USB / memory sticks).
- Attempt to bypass any security controls or configurations that have been implemented on school IT equipment or networks, or add to or remove hardware that has been provided by the school for business use.
- Use school equipment to transmit, store or distribute material which may be innapropriate or break copyright law (e.g. personal images of staff, music files, personal data relating to staff) or any other law or regulation.
- Allow anyone not employed by or working directly for the school to use the equipment or services provided.

- Attempt to use any systems or networks without authorised access.

Be AWARE that**:**

- Any school IT equipment may be removed for investigation at any time without notice.for court proceeding or for review by the school's IT Consultant.

6.2 Portable equipment – laptops, tablets, mobiles

Laptops, PDAs and other mobile computers are particularly subject to the risks of damage, loss and theft.

While all these devices **must** be encrypted to protect school information, losing a device is expensive and inconvenient.

Everyone MUST:

- Remember that they are responsible for the safe-keeping of any equipment given to them. The school continues to own the equipment.
- Check with their insurance provider that they are insured for loss or theft of any equipment which is on loan to them from the school when you are not at work.
- Make sure that any mobile computing systems are stored out of view when left unattended.

If staff leave, or no longer work for the school, any equipment **must** be returned to their direct line manager.

If the given equipment can make telephone calls or use data, **personal use should be prohibited**

If the equipment is going to be used abroad, **you must** inform your line manager.

7.3 Health & Safety

Everyone MUST:

- Ensure that any equipment is installed in a safe and stable environment.

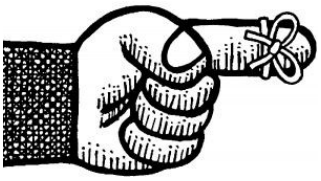
Access to Information*: Rule 6*

You MUST NOT:

- Remove the case, cover or attempt to disassemble or dismantle computer equipment in any way. If there is a problem, **report it** to the school's IT Consultant
- Move or lift any non-mobile computer equipment.

7 Keeping our systems secure

7.1 Background



- The school spends money and time trying to protect its sensitive information – much of which is about it's pupils, staff and parents. However:
- **REMEMBER:** Security starts and ends with **STAFF.**

7.2 Passwords

- To help **identify** staff to school systems, you will be given one or more *usernames* and *passwords*.

Managers MUST:

- Work with the school's IT Consultant to ensure that their business applications, or changes to them *integrate* with school security systems and policies. For instance, this can avoid staff having too many usernames and passwords to remember.
- Inform the school's IT Consultant immediately of staff leavers, moves and changes to ensure that people don't have access to information or resources when they shouldn't. This should be done using a leavers form.
- Take ownership and responsibility for managing user accounts on any 'cloud' services where those services are not integrated with central IT security systems.

Everyone MUST:

- Use a different password at work than you the ones you would use to access other sites on the internet (e.g. Facebook, web-mail)
- Use a different password when you're asked to change it.
- Follow best practice password standards – which currently require UPPERCASE, lowercase letters and either numbers or #Symbols!# to be used. Passwords should have a minimum length of 8 characters.
- Always lock your computer when you leave it, even if it is just out of sight. **Remember,** you are accountable for anything performed when you are 'logged in' and people can access information they wouldn't normally be able to.

You MUST NOT:

- Write down your username and password where it can be seen or found by others.
- Share your username and password with anyone else, **even if they say they need it, or are allowed to have it**.
- Let others use your computer unsupervised.

7.3 Protecting against malicious software and 'viruses'

School work relies on IT Systems operating efficiently.

A 'virus' on computers could result in:

- Systems not being available.
- Information being lost.
- Information passing to the wrong people, who aren't authorised to see it.

Whatever happens, **everyone** has a responsibility to be vigilant, and to use systems responsibly.

Everyone MUST:

- Report any warnings you see on computer systems which are used for work to the school's IT Consultant.
- Let the IT Consultant know if you think there is a security problem with any of the computer systems, networks, software or 'apps'.
- Use common sense when using school systems.

You MUST NOT:

- Attempt to introduce any software, 'virus' or similar to school computer systems.
- Attempt to bypass any security controls that have been implemented on IT equipment used for work or the school networks.

8 Working out of the school

8.1 Background

This rulebook is only applicable if your school offers remote working options

The school computer system offers a number of ways to allow people to work out of the school office.

Before doing so, you **must** check with your line manager on any policies and agreements that apply to you, and take any guidance on Health & Safety arrangements.

8.2 General principles

You MUST NOT:

- Allow other people, including family members, to use school-provided computer equipment.
- Allow other people, including family members, to use school applications or the services provided for school staff or members.

You MUST:

- Ensure that other people, including your family and friends cannot access the school information which you have been given access to to help you do your job.

All our policies and rules apply – regardless of where you are.

8.3 If we give you equipment

Be AWARE that**:**

- **It is your responsibility** to ensure the safe keeping of any equipment we give you, and to use it in line with the school policies and rules.
- **You MUST** report any theft of school equipment to your line manager, IT Consultant, the school's data protection officer immediately, together with a police reference number.
- **You MUST** report any damage to that equipment to your line manager.

8.4 If you are using your own equipment

→ Refer to our rule book on 'Bringing your Own Device' to work

8.5 If you are using a wireless network

Wireless networks can offer a flexible way to connect to the internet, but they also come with security risks.

Public or 'Guest' Wireless networks, sometimes known as *'hotspots'* can be convenient and are increasingly available in cafes, hotels, public buildings – and even on the street.

YOU MUST take care while using public wireless networks, and should not assume they are secure.

The following guidance does contain some technical language – but it's essential that you **understand** it, as it will protect **you and your personal data,** as well as our systems.

- Read the **terms and conditions** of the network – and don't use it unless you are happy to be bound by them.
- Use a **firewall** – software that protects you from other computers on the internet that may wish to attack you. If you have an iPad or another tablet – this is most likely covered – if you have a Windows or Mac – there is a firewall built in, or one will be installed with your antivirus – **but, check that it is turned on.**
- When you connect, if you're using Windows, you may be asked whether you are connecting to a 'Public' network – always select 'Public network', or people may be able to access your files.
- Make sure you keep your equipment up-to-date, applying patches, antivirus or manufacturer updates automatically wherever possible.
- Don't ignore any 'certificate warnings' you see when you're trying to access web sites – if your web browser (e.g. Internet Explorer) tells you there is a security problem, there is – and your information is at risk. Disconnect and go elsewhere.
- Turn off your wireless when you're not using it – apart from anything, it can save battery!

Remember: You may not be allowed to connect to school systems from any network unless your device is secure and up-to-date.

Private/Home wireless has fewer risks, but make sure a password is needed to access the network and that it is using ‘WPA2’ encryption. If your Internet service provider supplied a router, you can check with them.

9 'Bring Your Own Device'

Using your own computer, tablet or smartphone for work

This rulebook is only applicable if your school offers this as an option

9.1 Background

If approved by a school IT Consultant – you may use your own equipment to work with school information. You may also use mobile and wireless networks to connect to us.

This document applies to PCs, MACs, Tablets, Smartphones – and any other type of computer equipment you might use to access and work with school information.

However:

When you do this, you **agree** that you will only use the methods provided by the school's IT Consultant to connect and work with school information, and **agree** to follow the rules.

You also **agree** that the school IT Consultant may scan the device you use to determine whether it has any security problems, and that we reserve the right to refuse access at any time.

You **agree** that the school may apply 'policies' to your device which may result in changes being made – e.g. your device may be encrypted, or a password may be applied when it starts up.

9.2 Basic Responsibilities

When using school information and systems on personal equipment:

Everyone MUST:

- Still follow all school policies and rules. We'd like to also remind you about the school's Data Protection policy and the Code of Conduct.
- Accept personal responsibility for the safety of any school information held on their equipment.
- Take care to ensure that school information is not viewed by or accessible to unauthorised people.

You MUST NOT:

- Share your access to, or school information with anyone who is not authorised to see it – including family, friends, relatives, and acquaintances. *When the school gives you access it is given to only **YOU** as an individual.*

- Transfer school information to devices other than the ones you use to connect to us, as these will not have been checked for security, and may be set up in a way which is not suitable for working with school data.

Be AWARE that:

- **YOU** are **responsible** for maintaining your own equipment, patching it, keeping it up-to-date and ensuring that it runs appropriate security software (e.g. a major mass-market antivirus/firewall product on a PC). If you do not maintain your equipment, **you will not be allowed to use it.**

- If you fail to follow school policies and rules, disciplinary action may be taken.

- You will be held accountable for any incidents which compromise the safety of any school information held on your device.

- The school remains the owner of its information – regardless of its location.

9.3 Costs, Insurance and audit

Be AWARE that:

- When using your device for work, you remain liable for any costs incurred from using it. This includes support, repairs and data tariffs, including any costs you incur when 'roaming' abroad.

- **You are advised to** check that any insurance policies you may have cover usage for work purposes. The school cannot accept liability for loss, theft or damage to your device.

- By using your own equipment, you also give your agreement that, in the rare event that the school deems it necessary to conduct any investigation into misuse, fraud or other criminal activity, the school's appointed investigating officer may requisition or scrutinise your device for the purposes of that investigation.

9.4 Support

Be Aware that:

- The school **will** provide support for any software or application which it deploys directly to your device to help you in your work.
- (The below text varies depending on your school's normal processes)
- The school will not:
    - Provide hardware support for the device.
    - Provide support relating to the device's configuration, setup, performance, network connectivity or any other applications.
    - Be liable for any damage to the device, its hardware, software or data contained on it through using our services.

9.5 Device Configuration

Sometimes, the school needs to apply a 'security policy' to your device – *e.g. to make sure it is encrypted or has a password that must be entered before it can be used.*

You will be informed on screen if this is the case, and given the chance to accept the policy or reject it. You will not be able to use your equipment without accepting the policy.

You MUST:

- Agree that the school may enforce the relevant technical policies on your device before it can be used.
- Agree that the school may update or change these policies at any time.

You **MUST NOT:**

- Attempt to disable any security policies we apply to your device.

Be AWARE that:

- 'Jail broken', 'rooted', or 'hacked' mobile devices are not permitted to access our services, as we cannot trust that they are secure.

9.6 Your Privacy

Be AWARE that:

- In providing its services to you, the school will collect data on an on-going basis about the device you are using and its configuration. This will include – but not be limited to:
    - Its make, model, Operating System and version.
    - Applications installed.
    - Security configuration.
    - Telephone number & International Mobile Equipment Identity (IMEI) number *(where applicable).*

- This information is obtained to ensure the smooth running of the BYOD services.
- Additionally, the following information may be obtained as the device is used:

    - Traffic to/from school systems.
    - The device's location at any given time *(where applicable).*

    Such information is subject to the school's strict **monitoring policies**. In particular, **location information** shall not be made available in any circumstance, other than if:

    - The user reports their device as lost / stolen, and requests that information directly from the IT Consultant.
    - It forms part of any investigation into misuse, fraud or any other criminal activity.
    - The law requires us to disclose it.

9.7 Incidents, loss, theft & change of ownership

Everyone MUST:

- Report any suspected loss or theft of a personal device which has been used for work to the IT Consultat and the school's data protection team **immediately**.

- Obtain a police reference number for any theft and provide that to the IT Consultant and school's data protection team.

- Inform the school if you intend to resell or transfer your personal device to someone else, so that we can be assured that it has been wiped according to the school's protocols prior to the sale or transfer.

- Agree that, if you are using a tablet or 'smartphone', the school may wipe your entire device and/or the specific school information present if it is reported lost or stolen. *(varies from device to device).*
    - The school shall not be liable for any such loss of data.

10 The internet: Responsible usage

Background

The school recognises that the internet is now a major contributor to everyone's daily life, and wants its rules around usage to reflect that.

Tensions can arise at the school when the internet is used irresponsibly – when instead of helping with work, it gets in the way. We'd encourage you to read these rules carefully, and discuss any queries you may have with your line manager.

Your School's GDPR Lead may wish to apply supplementary rules or policies in your work-area. If they wish to do so, you will be informed in writing, and they will be responsible for ensuring that they are applied. You may have a named online-safety coordinator at your school (see above); this person may or may not be the designated safeguarding lead (DSL), but KCSIE makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."

This policy aims to help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the children and young people in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Access to Information*: Rule 10*

The Online-safety coordinator MUST: implement and document any local additional restrictions or policies.

NOTE that there is a separate rule book on social media sites – e.g. Facebook and twitter, which you must read if you intend to use such sites.

10.1 Browsing the Internet

When you use the internet (the 'Web') during work, the School **assumes** that you are using it to help you with your job.

You MAY also access it for your personal use – however;

This **MUST NOT** interfere with your work, affect your performance, or disrupt your colleagues.

This applies **regardless** of what equipment you are using, or wherever you are, if you are meant to be working.

The School **will** block access to sites on the internet which breach its rules, and put it, its information, or its staff and students at risk. Which sites are blocked are determined by the School's Network.

10.2 Our requirements

You MUST NOT:

- Deliberately **view**, **create** or **download** any content on the web containing material that:
    - is pornographic, sexual or obscene.
    - encourages breaking of the law – *e.g. extremist or terrorist material.*
    - breaks the law – *e.g. breaches copyright.*
    - is intolerant of others – *e.g. Homophobic; Racist, Religion intolerant.*
    - is potentially offensive to others – *beware, what does not offend you, may still offend other people.*
    - could cause damage to the School - *e.g. malicious software.*
- Post, or be involved in the posting of any information that could damage, or potentially be damaging to the interests of the School and their staff.
- Use your School's password(s) when registering on web sites.
- Use School credit cards online without the prior agreement of Financial Services.

Be aware that**:**

- The internet contains sites that are malicious, and can try to attack your computer. We advise that you **only browse sites you know**, or that you feel you can trust.
- If you are on a school computer, and a site shows any *security warnings*, or suggests that *'your computer has a virus'*, stop browsing immediately, and **report this to the School's IT Manager.**
- You should beware entering your personal details, or any **credit card data** into a site you do not know.
- If you feel that your computer has been attacked after visiting a web site, or shows strange behaviour – **report this to the School's IT Manager**.

Get Safe Online

We advise everyone who uses the internet – at work or at home - to visit **Get Safe Online** for more information.
www.getsafeonline.org

10.3 Audio & Video

Everyone MUST:

- Be sensitive to other people in the School who may not have the same level of interest in the material as you.

You MUST NOT:

- Use these resources excessively. Only use them for a limited time, and when required.
- Use the internet connection provided for the watching of online television, radio or listening to music. *If you want to listen to the radio – please buy a radio!*

Be AWARE that:

- Excessive use of these services that breaks these rules or causes disruption to the School will result in **your access being withdrawn**.

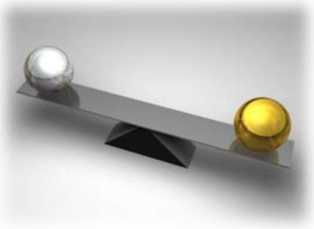
10.4 Rules on personal usage

Everyone MUST:

- Comply with the School's code of conduct, and **NOT** do anything which is not in the School's best interests.
- Comply with the law.

You MUST NOT:

- Allow personal usage of the internet to take priority over, or affect your work.
    - *Managers are responsible for working with their staff on any matters of performance, based on their delivery of work and achievement of agreed objectives.*



- Use your school e-mail address in online forms, or to subscribe to any non-business 'blogs', bulletin boards, newsgroups or e-mail services.
- run your own business ventures from work, without prior written permission from your line manager.

Be AWARE that:

- The School cannot guarantee the security of **any site** accessed on the internet, or the security of information transmitted to or from those sites. *This includes sites which are advertised in the browser as being 'secure'.*
- Your usage **of the internet is at your own risk.**
- The School reserves the right to monitor, log and report on all usage of the Internet. The School also reserves the right to block access to any site, user or device for any reason. **Access is a privilege which can be withdrawn.**

11 The internet: Social Media – Facebook, Twitter and Friends

11.1 Background

- The School acknowledges that Social Media sites – such as Facebook, Twitter and Instagram – are now a part of everyday life.
- We appreciate that many use them for everyday communication - replacing e-mails, text messages, or telephone calls.
- We also acknowledge that sites that provide 'instant updates' and 'instant messaging' can also be disruptive to people's work and break their concentration.
- The School has therefore decided to permit *responsible usage* of Social media sites, and reserves the right to put *controls* in place to manage this.
- **Everyone** needs to make sure that using these sites does not damage the School. Communication about the School **MUST** go through **official** channels.
- Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).
- Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.
- Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner

11.2 Do's and Don'ts:

You may:

- Access Social media sites in line with the School's rules on Responsible Usage of the Internet, unless your local management has put in place additional policies – of which you have been informed in writing.

Staff of the School MUST:

- Remember that using these sites must not interfere with your work.
- Take care and use common sense:
    - Staff are representatives of the School and are in the 'public eye' when they post online.
    - **Do not** post anything that could embarrass you or the School – offensive or inappropriate material, information, photographs, files etc.
    - **Do not** be 'friends' with or make a friend request** to any pupils, parents, contractors or otherwise communicate via social media.
    - **Avoid** posting personal data – your home address, phone numbers or anything that can be used to 'steal your identity'.
    - **Do not** upload any files which contain personal or sensitive data. i.e. photos of pupils or any third party relating to the School.
- If you wish to **post, or respond to ANY** information relating to the School, its business, your employment, its employees, pupils etc. **you MUST** seek advice from the School's official social media account manager, where issues of consent will be sought.

Staff MUST:

Be aware of their responsibilities and must pay attention to what they post on any Social Media sites.

GET SAFE ONLINE .org

Get Safe Online

We advise everyone who uses the internet – at work or at home - to visit **Get Safe Online** for more information.
www.getsafeonline.org

12 Sending messages – E-mail 'School Messenger'

12.1 Background

E-mail and other services offered by the School, i.e.

- LGfL or School email;
- School messenger Communicator

can offer an efficient way for people to communicate both inside and out of the school.

The School provides these systems **for business usage only**, as:

- Any email or message sent may be considered as a public record – it may be disclosed under the Freedom of Information Act;
- The School may archive any or all messages for the purposes of such disclosure for a period of time;

The school allows access to web-mail systems (e.g. Hotmail, Google Mail) if people wish to send personal mails. These **MUST** be used in line with the School rules on responsible internet usage.

The School also provides **secure mail** systems that **MUST** be used to send sensitive and personal information.

12.2 Basic responsibilities

You MUST:

- Keep messages precise and to the point. Be polite and respectful to the receiver.
- Remember that others may need to be able to read your work e-mails when you are on leave or off sick. Discuss **delegated access** with your manager if appropriate.

You MUST NOT:

- Use the services to distribute any material that:
    - Is pornographic, sexual or obscene.
    - Encourages breaking of the law – *e.g. extremist or terrorist material.*
    - Breaks the law – *e.g. breaches copyright.*
    - Is intolerant of others – *e.g. Homophobic; Racist, Religion intolerant.*
    - Is potentially offensive to others – *beware, what does not offend you, may offend other people.*
    - Could cause damage to the School or another person or organisation - *e.g. malicious software.*

- Post, or be involved in the posting of any information that could damage, or potentially be damaging to the interests of the School.

- Send messages that might make the School legally liable, if you do not have the authority to do so.

12.3 Keeping safe

You MUST:

- Take care - Messages can contain attachments or web links that can cause you problems or damage our systems. Ask yourself:
    - Do I know who has sent me this message?
    - Was I expecting to receive this file or web link?

- If the answer to one of the above is 'no', think twice before opening the message, any attached files, or clicking on links.

You MUST NOT:

- 'Auto forward' your School e-mail account to a web-mail account, or an account at another organisation, as we cannot offer any guarantees that this is secure.

12.4 Forwarding

- Use remote access if you need to access your mail from elsewhere, don't try to forward it automatically to another mail account.

Get Safe Online

We advise everyone who uses the internet – at work or at home - to visit **Get Safe Online** for more information.
www.getsafeonline.org

12.5 Responsible usage

You MUST NOT:

- Copy-in excessive amounts of people to messages, or send to 'all staff' distribution lists unless you have been authorised to do so.
    - *What is important to you may not be important to everyone, and may cause offence!*
- Use messages to send large files to an extensive distribution list.
- Send credit card details in messages.

12.6 Monitoring & Manager access

Be AWARE that**:**

- The School reserves the right to monitor all usage of webmail, School e-mail and School Messenger services as per the School's monitoring procedures.
- In your absence, if you have not delegated access, your line manager may need to access your mail account to keep the business running.

12.7 Secure e-mail

You MUST NOT:

- Use the School's e-mail system to send personal or sensitive business data out of the organisation, without using a **secure e-mail systems**, unless the risk of not sending the information immediately could place someone at risk.

Details of secure mail are available from the **The School's Data Protection Service** and/or your manager.

13 Using School Telephones, Mobiles & Voicemail

13.1 Background

These rules apply to any kind of telephone provided by the school – whether that is a desk phone in the school, a cordless phone or a mobile.

They don't apply to applications and internet access on phones. That is covered in other **rule books**.

Everyone MUST:

- Conduct telephone calls in a business-like and professional manner.

You MUST NOT:

- Attempt to use any unauthorised device with the school telephone systems.
- Engage in an argument if the person on the other end of the phone is abusive to you. Politely tell them that you will not continue the conversation if they continue to be abusive, hang up and report the incident immediately to your line manager or appropriate contact.
- Use adult phone lines, chat lines or any premium rate or 0990 numbers.
- Use international numbers, or roaming when using the phone outside the UK.
- Under normal circumstances use the phone for making personal calls. Personal calls should be for making a call in an emergency or occasional use, for example to call home today if late.
- Ever use the phone to communicate material which:
    - Is offensive – including pornographic, racist or sexual material.
    - Is libellous.
    - Is criminal, or could cause the law to be broken.
    - Is extremist, or terrorist.
    - Is damaging or potentially damaging to the interests of the school.
    - Could be perceived as bullying or harassment.

Be AWARE that**:**

- The school reserves the right to ask for payment for personal calls from the nominated owner of the device/extension.
- The school will be monitoring usage, investigating any significant usage and may perform spot checks on individual bills.

13.2 "Desk phones" in the school office

Everyone MUST:

- "Sign in" to your phone when you come into the school office. (If applicable)
- Only use a desk telephone for personal reasons, where exceptional circumstances require it (i.e. you have no access to any non-school phone or payphone, and a short call must be made with urgency).
- Keep personal calls to a minimum.
- "Sign out" of your phone when you leave the school office. (If applicable)

13.3 Mobile Telephones, iPhones and 'smartphones'

The school may provide mobile telephones to a wide range of its staff. Many of these phones – such as iPhones are 'smartphones', which can access the internet and run 'apps' – small programs which can help with work.

This rule book sets out the rules on general usage of these devices – however, you **must note** that smartphones are considered as **computers** in our rules, and therefore **all relevant rules which apply to computer usage also apply to these devices**, including the school's right to audit their use.

Users of mobile phones therefore **AGREE** to use them in line with the entire Access to Information policy and Rule Book. Also;

Everyone MUST NOT:

- Make personal calls to premium rate or international numbers or during roaming (using the mobile phone outside the UK).

Everyone MUST:

- Declare personal and business calls made using a school mobile telephone so that personal calls can be recharged to you.
- Note that, as part of the billing process, managers can see basic details on calls made, including destination, time and cost.
- Comply with current UK law for mobile use. This includes the restrictions on using a mobile phone while driving.
- Keep the mobile phone that has been issued to you safe. You must report any loss, theft or damage immediately.
- Lock your phone when not in use with a PIN number, password or lock code. This will often be enforced by the school – *you must not attempt to disable it or any other security control.*

- Ask their manager before using a school mobile telephone abroad *(including the Isle of Man and the Channel Islands).*
    - Service may not be available to you outside of the UK unless a request has been submitted to the school's IT Consultant.
    - You will be billed for any additional charges for calls or data.
- "Subscription services" can be particularly expensive. They typically require you to text a code (e.g. 'GAME01') to a particular number (e.g. 7000) to download a game, ringtone or horoscope, and often have a recurring cost.
    - You **MUST NOT** use these services on devices provided to you – and any usage will be considered as personal usage and recharged to you at full cost.

Additionally, **You MUST NOT:**

- Send any sensitive school information via instant messaging tools such as SMS (Short Message Service), MMS (Multimedia Messaging Service), Whatsapp etc.
- Install inappropriate applications (apps) on your device.

14.4 Voicemails

Voicemail services are provided for school use only. Private messages may be left, but these should be kept to a minimum and discouraged.

Everyone MUST:

- Use voicemail in a way that is business like and professional.
- Use voicemail outside working hours to take messages.
- Check your messages regularly.
- When recording your outgoing message:

  - **Do** be clear, polite and concise.
  - **Do** state your name and service unit.
  - **Do** keep your message up-to-date.
  - **Do** offer to return people's calls where appropriate.
  - **Do** give out details of an alternate contact who can deal with urgent issues.

You MUST NOT:

- Use voicemail unless it is for a short, specific period or time.
- Use voicemail to store credit card details, or information about payments.
- Use voicemail for when your phone is busy if it is possible to divert to another colleague instead, with their agreement.
- Use voicemail during working hours on personal and service extensions where staff are intended to be present to take calls from the public, unless it is for a strictly limited time with a specific purpose.

Be AWARE that**:**

- Usage of all school telecommunications systems are monitored.

14 Reporting Incidents and 'near misses' (Data Breaches) – your responsibilities

14.1 Background

Everyone MUST ensure that incidents which might affect the security of our information, our systems or those of our partners are reported as soon as they are aware, and to the right people – The School's Data Protection Officer. It is a legal requirement to for the School's Data Protection Officer to report any appropriate incident to the Information Commissioner's Office within 72 hours of anyone becoming aware.

14.2 Incident types

An incident might be:

- Your PC behaving unexpectedly; a Virus.
- Loss or theft of information or something on which information is stored - accidental or otherwise.
- Loss or theft of mobile devices.
- Loss or potential loss of personal information.
- Personal information disclosed in error.
- Excessive personal information disclose.
- Information sent to the wrong person.
- When someone can or has accessed information without being authorised to do so.
- Someone trying to make you give out information which they're not entitled to receive.
- An unauthorised device on the school network.
- Criminal damage.
- A problem affecting the place in which information is stored – fire, flood.
- Abuse of our information systems and computers.
- A problem where information or data suddenly is no longer 'fit for purpose'.
- Accidental viewing of a web page which causes offence.
- Receiving 'junk mail' in your e-mail.
- Loss of access to any system that stores personal information.

Everyone MUST

- Report an incident **as soon as you are aware of it.**
- Report the incident to the schol's 'Data Protection Officer' (school.dpo@brent.gov.uk) , the school's IT Consultant, or the school's GDPR Lead who must inform the School's Data Protection Officer. This can be done using the School's data breach notification form.

15 Cloud Services – School Approved, Go4Schools, OneDrive, Google Drive, etc.

15.1 Background

Today, hundreds of services are available on the internet ('in the cloud') which can help us in our everyday lives and with our jobs. The school can't guarantee that these services are secure – but understands they can be useful to us.

Some, like Google Drive and Dropbox are services which can be bought and used by anyone to make notes and store files. Many have 'apps' that can be used on a smartphone. Web-mail is also a "**personal cloud service"**.

The school may also buy **enterprise cloud services** – where a company on the internet provides a full service to us.

This document sets out the rules for both **staff** and **managers** within the organisation on using cloud services of **both types.**

15.2 For ALL STAFF: Personal Cloud Services

You may access these services on the internet, subject to the following rules:

You MAY:

- Access these services for personal use, as covered by the school rules on using the internet.
- Use the services to assist you in your work – for instance, for taking notes, if your line manager agrees in writing or local policies.

You MUST NOT:

- Store sensitive information on these services – especially **personal information**, and information marked as **Official** or **Official-Sensitive**.
- Use them as the main place where school information is stored.
- **Use a personal cloud service that transfers or stores personal data outside the UK. Currently this includes Dropbox.**
- Use them to share files or information with members of the public, other staff or parents. The school offers secure mail and secure ways of sharing files – ask the school's IT Consultant.

15.3 **For School Business Managers / and GDPR Leads:**

15.4 **You still remain responsible for the information stored on the system, controlling and removing access to it, and any problems with its security, accuracy or availability.**

You MUST:

- Contact your IT Consultant **before** procuring any cloud service.
- Contact the School's Data Protection Team and complete a Data Protection Impact Assessment Questionnaire in order to assess the risks.
- Send the vendor the consensus assessments initiative questionnaire v3.0.1 (You can request this from the School's Data Protection Team)
- Know, or can find out some of the services available to you which have been 'tried and tested' by other schools.
- Know the other services being used in the school – you may be able to use an existing one and save money.
- Help to make sure the services you buy will actually work on school computers, tablets etc.
- Log which cloud services the school are using – as they're accessed across the internet, it's important to make sure the internet connection is robust.
- Understand how cloud services can integrate with the school's internal IT systems and networks – *e.g. do you really want to give your staff another username and password to access the service – and are you happy to maintain a separate database of your staff yourself?*

Access to Information: *Rule Book Supplement*

A. How the school applies its rules

How to obtain an exemption to a rule

A.1 Background

The school has developed these rules to protect its pupils, staff members, business partners, and the services it offers.

It takes these rules seriously, and expects that anyone accessing or working with school information will do likewise.

This section discusses:

- How you can get further information about the rules.
- How to get an exemption to a rule.
- What will happen if a rule is broken.

A.2 Informing you about the rules

The school notifies you about its rules:

- When you log into the school systems.
- Via the online training courses.
- Via your line manager.

School Business Managers are responsible for ensuring that all their staff have reviewed and agreed to the rules.

If you would like further information, or would like to clarify any of the rules, you should contact:

- **Your Line Manager.**
- **The School's Data Protection Team.**

A.3 Seeking exemptions

Anyone has the right to seek an exemption to this policy, as long as it is for a justifiable purpose.

To seek an exemption **you MUST** log a call with the school's IT Consultant.

- State your business case in the call.
- Give the name of a manager who supports the exemption.

This also applies to any requests to bypass web filtering etc.

Objections to any of the rules should also be raised as above.

A.4 What will happen if a rule is broken?

If a rule is deliberately broken or ignored, then the school will consider it as a breach of policy. It may also be a breach of the school's Code of Conduct.

If a rule is broken, a full investigation will be carried out. This may result in:

- Restriction / Removal of services;
- Disciplinary action;
- Legal Proceedings;
- Reporting to an appropriate standards body, internal or external;
- Reporting to another agency.

Investigations will be conducted formally, and actions taken will be tracked.

As part of an investigation, access to a user's login, e-mail, network shares, telephone records, files and equipment may be required.

The monitoring of communications by the authority is authorised under the "Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000" which came into force on 24th October 2000 under the Regulation of Investigatory Powers Act 2000 (RIPA), and our process is compliant with the Human Rights Act 1998.

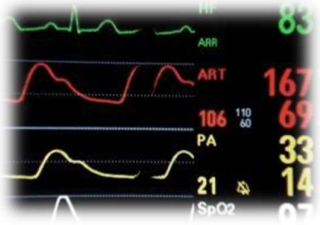
As a user of school systems, you are informed of our monitoring via the rules and this document.

Further details of monitoring can be found in Rule Book Supplement B.

B. How the School Monitors Usage of its Information Services

How this affects you.

B.1 Background



The school monitors the use of its systems and networks to protect itself, the people who work for it, the information and systems of the school, and our business partners. Monitoring information includes information on the school's network and information belonging to the school in many forms, including access logs, emails, documents and communication

B.2 What we monitor for

The school reserves the right to monitor all its systems and user activity, specifically to detect:

- Unusual user activity that might indicate a problem – such as potential fraud, criminal activity, a breach of these rules, or a breach of the code of conduct.
- Whether there are problems with the school's systems and networks.
- Whether information is passing to people who are not authorised to have it, or when it is being copied or passed on to systems on which it should not be stored.

Routine maintenance and housekeeping procedures may also detect issues of the type above which will be raised according to the rules in this supplement.

Monitoring is **NOT** used to measure or report on staff performance – this is the responsibility of line managers.

Line managers are responsible for working with their staff on any matters of performance, based on their delivery of work and achievement of agreed objectives.

When staff are leaving the school, an 'out of office' and a suitable message should be set. The school's IT Consultant can set up an 'out of office' if a person has left already. Line managers should not use monitoring for access to emails sent to staff that left the school unless there are exceptional circumstances.

Monitoring information which can identify an individual's location will **NOT** be released unless as part of a formal investigation by Audit & Investigations or law enforcement. It should not be relied on for purposes of Health & Safety.

This information applies solely to services directly provided by the school, and does not apply to third party services – e.g. cloud services, mobile networks

B.4.3 Authorising the release of monitoring information

The process which IT Consultant will follow is documented here for the sake of openness and for reference.

B.4.3.1 **Receipt of Request**

On receiving a request, the notified manager ('incident owner') will:

- Inform the school's IT Consultant of the request.
- Attach a copy of the request to the raised IT Consultant message.
    - The copy should be **protected** from unauthorised opening with Egress. Access should be restricted to the Digital IT Consultant and the requestor.
    - No information should be placed unencrypted in the call log, or in a format that reveals the details of the requestor or the subject(s) of the request.

B.4.3.2 **Assessing the request**

The incident owner must assess the request to ensure that it is from an authorised individual:

- By checking with HR that the person named is the manager or ultimate manager of the members of staff on whom information is being required.

- If it is for the purpose of determining whether:
    - A user has broken the code of conduct.
    - A crime or breach of legislation may have occurred, or is likely to occur.
    - It is related to the investigation of a related issue or incident to which the information is relevant, in the context of the issues above.
- Requests the minimum amount of information to prove a case in respect of the terms above.

If the request meets the terms above, the incident owner should **accept** the request, and inform the recipient that their request will be processed. The incident owner should seek clarification on any issues which are uncertain, outline what will be provided, and by when.

If the request does not meet the terms above, it should be rejected, and the person requesting informed as to why.

Any changes or actions taken should be logged to the service call, and protected with Egress as above.

B.4.3.3 **Providing information**

- Before information is provided, it **must** be reviewed by the School's Data Protection Team to ensure that it is proportionate, and to allow for redaction to ensure that the terms of the Data Protection Legislation/the General Data Protection Regulation are being followed.
- A suitable method of access will be provided to ensure that access to the information is on a need to know basis and that access to other confidential information is prevented.
- It is a disciplinary offence to release monitoring information which can identify an individual's location unless as part of a formal investigation by Audit & Investigations or Law Enforcement.
- If the School's Data Protection Team redacts information, an explanation must be given as to why the information has been removed or not provided.
- The information provided must be logged to the call, protected with Egress. The same information should be sent to the requestor, with rights given to them to access it.

- **The School's Headteacher must authorise the release of any information.**

B.4.3 Requesting monitoring information

As a manager, it is your responsibility to ensure you **understand** the information provided before you take any action, disciplinary or otherwise.

If you do not fully understand the information provided, **you must** consult the School's Data Protection Team.

Access to Information: Declaration

16 Third Party Declaration

In order to access and use the school's information systems, including both computer systems and physical files, we ask you to read the School's Access to Information (version 1 – September 2019) in full and then sign this declaration as your commitment to abide by its rules. This is in addition to any other school policies and procedures that you are required to follow. Before signing any areas of uncertainty, it should be discussed with a line manager and the school's Data Protection Office.

Third parties and contractors should return the signed declaration to the person who has authorised their access to school information systems. This declaration will be stored for as long as you have access to the school's information systems. You will be notified of changes to this policy.

17 Declaration

- I have read, understood and agree to abide by the school's Access to Information Rule book (version 1 – September 2019).
- I am aware that any breach of this policy could lead to the school's information systems being withdrawn or further action, including instigation of legal procedures being taken.
- I will report to the school's IT Consultant immediately if I suspect or know of any information security problem.

Signed: _____ **Dated:** _____

Name: _____

School: _____

Line Manager: _____