GREAT FINBOROUGH CHURCH PRIMARY

Information Management Policy

Linked documents:
Online Safety Policy
Data Protection Policy

Prepared by:	H Elliss
Approved by:	WGB
Signature of Chair of Governors:	Jamie Warner
Status & review cycle	As required
Date approved:	14.06.18
Review date:	As required

Contents

1. Aims
Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

3. Roles and responsibilities
This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 Data Protection Officer
The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body and, where relevant, report to the body their advice and recommendations on school data protection issues.

The Data Protection Officer is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our Data Protection Officer is Sian Durrant (Schools' Choice) and is contactable via:

- Landline: 01473 260741
- Mobile: 07720208841
- Email: sian.durrant@schoolschoice.org

3.2 Headteacher
The school is deemed to be a data controller and the Headteacher acts as the representative of the data controller on a day-to-day basis.

4. Use of Mobile Devices
This policy applies to all employees who use a mobile device for school purposes, both those owned by the School and personal devices (additional constraints apply to personal devices, see Bring Your Own Device below). It applies to use of the device both during and outside your normal working hours and whether or not your use of the device takes place at the School. This policy applies to all devices which are used to access the School's IT resources and communications systems, which may include smartphones, mobile phones, tablets, laptops etc.

When you access the School's systems, you may be able to access data about the School and our pupils, parents, contractors or suppliers, including information which is confidential or otherwise sensitive. When you access the School's systems using a device, the School is also exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to the School's systems or data), the threat of malware (such as viruses, spyware or other threats that could be introduced via a device) and the loss, wrongful disclosure or unauthorised alteration or deletion of School data (which could expose the School to the risk of non-compliance with legal obligations relating to confidentiality, data protection and privacy).

The purpose of this policy is to protect the School's systems and data and to prevent School data from being deliberately or accidentally lost, disclosed, deleted or altered, while enabling employees to access the School's systems using a device.

4.1 Device Monitoring
The content of the School's systems and data is the property of the School. All data, information and communications, including but not limited to e-mail, telephone conversations and voicemail recordings, instant messages and Internet and social media postings and activities, created on, transmitted to, received from, or stored or recorded on a device during the course of the School's business or on the School's behalf is the School's property, regardless of who owns the device.

The School reserves the right (remotely or otherwise) to inspect, monitor, intercept, review, disclose, remove or destroy all content on the device that has been created for or on behalf of the School and to access applications used on it for this purpose. This includes the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, printing, removal, destruction or deletion of transactions, messages, communications, posts, log-ins, recordings and other uses of the device. It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, employees should have no expectation of privacy in any personal data on the device. Employees are advised not to use the School's systems for communications of a sensitive or confidential nature because it is not guaranteed to be private.

The purposes for such monitoring are:

- to promote productivity and efficiency
- to ensure the security of the School's systems and their effective operation
- to prevent misuse of the device and protect School data
- to ensure there is no unauthorised use of the School's time or systems
- to ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
- to ensure that employees do not use the School's facilities or systems for any unlawful purpose or activities that may damage the School's reputation
- to ensure there is no breach of confidentiality or data protection.

The School may also store copies of any content for a period of time after it is created and may delete such copies from time to time without notice.

4.2 Disciplinary Action
Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the School's disciplinary procedure. Breach of this policy may also lead to the School revoking your access to its systems, whether through a device or otherwise.

Employees are required to co-operate with any investigation into suspected breach, which may involve providing the School with access to the device and any relevant passwords and login details.

5. Using Your Own Device
The School recognises that many employees will have their own personal mobile devices (such as smartphones and tablets) which they could use for School purposes and also that there can be benefits for both the School and staff in permitting such use. However, the use of personal mobile devices for school purposes can give rise to an increased risk in terms of the security of the School's IT networks and communications systems, the protection of confidential or otherwise sensitive information and compliance with legal obligations, such as data protection requirements.

With the prior permission of the Business Manager, employees may use a personal mobile device for school purposes, provided always that they adhere to the terms of this policy. However, employees are not required to use their personal mobile device for school purposes if they do not wish to do so. Personal devices will have access limited to allow access to the internet, including school email, but not other school systems.

NOTE: All conditions in Section 4 of this policy also apply to personal mobile devices.

5.1 Connecting Personal Devices to the School's Systems

Connectivity of all devices, personal and School, is managed by the Business Manager, who must approve each device as providing an appropriate level of security before it can be connected to the School's systems or network.

The School's Online Safety Policy will also apply as appropriate to the device.

5.2 Personal Device Monitoring
All monitoring arrangements as described in section 4.1 also apply to personal devices.

By agreeing to use your personal mobile device for School purposes, you confirm your agreement to such inspection or monitoring and to the School's right to copy, erase or remotely wipe the entire device, including any personal data stored on the device. Although the School does not intend to wipe personal data, it may not be possible to distinguish all such information from School data. You should therefore regularly backup any personal data contained on the device.

You also agree that you use the device at your own risk and that the School will not be responsible for any loss, damage or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of the device, its software or its functionality.

You must co-operate with the School to enable such inspection or monitoring, including providing any passwords or pin numbers necessary to access the device or relevant applications.

The School shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless absolutely necessary. If such copying occurs inadvertently, the School will delete such personal data as soon as it comes to its attention.

5.3 Security Requirements
You must:

- install any anti-virus or anti-malware software at the School's request before connecting to its systems and consent to the School's procedures to manage the device and secure its data, including providing the School with any necessary passwords
- keep the device's operating and security system and settings current with security patches and updates

If you download emails from your school email address onto your device you must:

- protect the device with a pin number or strong password, and keep that pin number or password secure at all times. If the confidentiality of a pin number or password is compromised, you must change it immediately
- ensure that access to the device is denied if an incorrect pin number or password is input too many times and ensure that the device automatically locks if inactive for a period of time
- at all times, use your best efforts to physically secure the device against loss, theft or use by persons who have not been authorised to use the device. You must secure the device whether or not it is in use and whether or not it is in your current possession. This includes passwords, encryption technologies and physical control of the device
- prohibit use of the device by anyone not authorised by the School, including family and friends
- delete emails promptly and only retain them for the minimum time required
- not backup the device locally or to cloud-based storage applications where that might result in the backup or storage of School data and any such backups inadvertently created must be deleted immediately

If the School discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, it shall immediately remove access to its systems and, where appropriate, remove any School data from the device.

In the event of a lost or stolen device, or where you believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must report the incident to the Business Manager immediately. Appropriate steps will be taken to ensure that School data on or accessible from the device is secured, including emails utilising your school email address. Although the School does not intend to wipe personal data, it may not be possible to distinguish all such information from School data.

On termination of employment, on or before your last day of employment by the School, all School data (including work e-mails) must be removed from the device. This must be evidenced to the Business Manager. You must provide all necessary co-operation and assistance to the Business Manager in relation to this process. The same process will apply if you intend to sell the device or to return it to the manufacturer or take it to a third party for repair or replacement.

5.4 Costs
You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase, repair or replacement costs. You acknowledge that you are responsible for all costs associated with the device and that your School usage of the device may increase your voice and data usage charges.

6. Use of Memory Sticks and other Portable Storage Devices
Use of personal memory sticks and personal portable storage devices to hold personal School data is not allowed. Wherever possible data to be transferred between staff should be saved onto the School's NAS drive and accessed from there. Where this is not possible an encrypted memory stick supplied by the school must be used.

7. Clear Desk Policy
The School is working towards a clear desk policy for all employees for the following reasons:

- it reduces the threat of a security breach as passwords and other confidential information are locked away or otherwise securely stored
- it ensures compliance with data protection requirements because personal data must be held securely at all times
- it protects employees' health and safety by reducing the risk of workplace accidents
- it reduces the risk of damage or destruction to information in the event of a disaster such as a fire or flood etc.
- it portrays a professional image to our parents, visitors and suppliers when they visit the School's premises

7.1 CDP Procedure
NOTE: This is the procedure for when CDP is adopted in full. In the interim period staff must comply with as much of this procedure as is feasible.

At the end of your working day or where you leave your workplace for an extended period during the day, you must tidy your workplace and tidy away all school-related paperwork and files into your desk drawer, filing cabinet or cupboard in an efficient and organised manner. These should then be locked overnight where locking facilities are available. Confidential information or information containing personal data must always be securely stored. If you are unsure of the information's sensitivity, either ask your manager or lock it away securely.

Put any paperwork that you no longer need in your rubbish/recycling bin on a daily basis. Please use the School's shredding facilities or confidential waste bags where the information in the paperwork is confidential. Any unwanted paperwork that contains personal data or sensitive information should be shredded. Paperwork that you do need should be acted upon and then appropriately filed.

This policy includes removable storage media which may contain files downloaded from your computer, such as memory sticks, portable hard drives and CDs. Media of this type must also be cleared from your workplace before you go home.

Additionally, this policy is designed to reduce the amount of paper that the School uses, which in turn reduces the amount of printing costs and filing space needed. You should not print out hard copies of e-mails or documents just to read them unless this is really necessary. All information stored on the School's computer and e-mail systems are backed-up so you will not lose the information unless you have specifically deleted it.

When printing out information, it should be cleared from printers immediately, particularly if the information is confidential or contains personal data. Faxes should also be taken from the fax machine immediately. Nothing should be left lying on printers, photocopiers or fax machines at the end of the day.

Finally, the floor space around/in your workplace should remain tidy and free from obstructions at all times.

It is your personal responsibility to adhere to this policy. If you fail to comply with the above rules, it will be dealt with in accordance with the School's disciplinary procedure.

8. Governor and School Staff Use of Email

The school provides e-mail and internet access to authorised users. The use of email within a school is an essential means of communication for staff, governors and students. In the context of school, emails should not be considered private and individuals should assume that anything they write or email could become public.

The purpose of this policy is to outline the procedure and protocols to be used when emailing and this policy must be adhered to by all authorised users.

8.1 Email Accounts

The school gives some staff and governors their own email account, using a school domain name, as a work-based tool.

This school email account should be the account that is used for all school business, i.e., forward facing communication with external parties. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal contact information being revealed.

NOTE: *Governors may use personal email accounts for correspondence between them and between them and the school, but should always use a school email account if communicating to third parties. Governors need to be aware of implications for confidentiality of their communications and where sensitive papers are involved they should be communicated by Governorhub rather than email.*

If necessary, email histories can be traced through the webmail system.

The following rules will apply:

- Under no circumstances should staff or governors contact students, parents or conduct any school business using any personal email addresses.
- It is the responsibility of each account holder to keep their password/s secure.
- If any issues/complaints are involved then staff sending emails to parents, external organisations, or students are advised to cc the headteacher.
- *The school requires a standard disclaimer to be attached to all email correspondence, clarifying that any views expressed are not necessarily those of the school. Please note that this disclaimer is automatically added to emails sent externally.*
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act or a Subject Access Request in certain circumstances.

Staff are expected to manage their staff email account in an effective way as follows:

- Delete all emails of short-term value.
- Organise email into folders and carry out frequent house-keeping on all folders and archives.
- Respond to emails in a timely fashion.

- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the relevant school policies, e.g., online safety apply.

Staff must immediately inform the Headteacher or Business Manager if they receive an offensive email and any suspicious emails should be reported to the Business manager and should not be opened.

8.2 Sending Emails

The following rules apply:

- When composing your message to a parent or non-staff member you should always use formal business like language.
- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please see the section below 'Emailing personal, sensitive, confidential or classified information'.
- Use your own school email account so that you are clearly identified as the originator of a message (if using the school Egress account ensure you sign your name at the bottom of the email).
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send whole school emails unless essential for school business.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

8.3 Receiving Emails

The following rules apply:

- Check your email regularly.
- If appropriate, activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source. If unsure, always consult the Business Manager first.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

8.4 Emailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data without the use of encryption is strictly prohibited. Users should ensure that they have read and are aware of the school's Data Protection policy.

The school has an Egress account that should be used for all secure emails other than those sent in response to an encrypted Office 385 email from the Local Authority.

If for any reason you cannot avoid using your school email to transmit such data, send the information as an encrypted/password protected document attached to an email, (if you are unsure as to how to complete this, please speak to the Business Manager) and provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone.

Always exercise caution when sending an email containing personal, sensitive or confidential information and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information.
- Verify (preferably by phoning) the details of a requestor, if unknown, before responding to email requests for information.
- Do not copy or forward the email to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify.
- Send the information as an encrypted/password protected document attached to an email. If you are unsure as to how to complete this, please speak to the Business Manager.
- Provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone.

- Do not identify such information in the subject line of any email.
- Request confirmation of safe receipt.
- When sending an email containing personal or sensitive data, the name of the individual is not to be included in the subject line and the document containing the information must be encrypted.
- To provide additional security you need to put 'CONFIDENTIAL' in the subject line and as a header in the email and any attachments to the email.

9. Monitoring arrangements

The Data Protection Officer is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice.

Otherwise, or from then on, this policy will be reviewed biennially or as required by changes in legislation.
.