Petersfield Church of England (Aided) School

DATA PROTECTION AND INFORMATION MANAGEMENT POLICY (GDPR)

Version	New GDPR Policy
Policy Type	FGB
Discussed by staff	April 2018
Approved by the Headteachers	April 2018
Adopted by the FGB	3rd May 2018 Updated (Resources) June 18
Next Review	Summer 2019

Petersfield Church of England Aided Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

A Management Information System (MIS) is a system to facilitate information flows in an organisation. MIS gives the opportunity to analyse and store information, within agreed procedures to minimalise bureaucracy and clarify process. In writing this policy, we have referred to guidance from ICT Service (Cambridge). To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the European General Data Protection Regulation (2018).

In paraphrase, the Regulation is based on six regulations, or rules for 'good information handling', which require personal data:
1. is processed fairly, lawfully and in a transparent manner
2. is used for specific purposes, explicit and legitimate purposes. Must have a legal basis for processing, which carry different rights to erasure and portability. Data can be obtained for reasons for contract; legal obligation; vital interest (safety); public task (official function); legitimate interests
3. is used in a way that is adequate, relevant and limited
4. is accurate and kept up to date
5. is kept no longer than is necessary
6. is processed in a manner that ensures appropriate security of the data.

The Regulation also sets out seven rights:
1. the right to be informed
2. the right of access
3. the right of rectification
4. the right of erasure
5. the right to restrict processing
6. the right to data portability
7. the right to object

All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy and Management Information Systems policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Protection Officer
Our data protection officer is Laura Penrose.

Responsibilities of Staff / Data Processors
All staff are responsible for:

1. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
2. Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
3. Handling all personal data (e.g. – pupil attainment data) with reference to this policy. Where data is requested the purpose of that information is stated and ensure, where possible, that the information gathered is accurate.
4. Teacher Trainees / Parent Helpers / Governors may be provided with less information than school staff but are still required to adhere to this policy and those associated with it.

Data Security
All Data Processors must follow the Acceptable Use Policy (appendix to this document) and take particular note that:

1. All personal data that they hold is kept securely and should not be left in public areas where there is general access.
2. Personal information is not disclosed either orally or in writing or via webpages or by any other means, accidentally or otherwise, to any unauthorised third party.
3. Personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) is treated accordingly.
4. All portable electronic devices used for storing personal data on school business (including privately owned equipment) should be kept as securely as possible on and off school premises.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information must:

1. Be kept in a filing cabinet, drawer, or safe in a secure office, or;
2. If it is computerised/electronic, be password protected both on a local hard drive and on a network drive that is regularly backed up. If it is sensitive personal data, strong passwords should be used, i.e. at least eight characters long and containing a mixture of letters/symbols/numbers. Passwords should be changed regularly and different passwords used for separate systems and devices.
3. If a copy is kept on a USB memory stick or other portable/removable storage media, that media must should be password protected, as above, and fully encrypted and/or kept in a secure filing cabinet, drawer, or safe. This is particularly important if they are taken from school premises.

Sharing Data
The school holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing. This information includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information. From time to time schools are required to pass on some of this data to LAs, the DfE and to agencies that are prescribed by law, such as Ofsted.

When considering sharing personal data, staff are responsible for making sure they are allowed to share it; and ensuring that adequate security (taking into account the nature of the information) is in place to protect it.

Rights to Access Information
All staff, parents and other users are entitled to:

1. Know what information the School holds and processes about them or their child and why.
2. Know how to gain access to it.
3. Know how to keep it up to date.
4. Know what the School is doing to comply with its obligations under the 2018 Regulation.

The School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 2018 Regulation to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing as per the Subject Access Request form which can be found in Appendix 4 of this policy. The School will ask to see evidence of identity, such as a passport or driving licence, before disclosure of information.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the 2018 Regulation

Other Policies

This policy is to be read alongside our Data Retention Policy, Breach of Data Protection Policy, E-Safety Policy, Privacy Notices and Information Asset Register.

Appendix 1 – Acceptable Use for Data Processors (adult)

A: Use of school based equipment and services

Access to school equipment, the school network and the internet

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any breach of security to the E-safety coordinator/Headteacher.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety coordinator.
- I will seek written consent from the E-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I understand that my files, communications and internet activity may be monitored.

Creation, storage and security of digital content

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car unattended or left in sight when not in use, e.g. by an open window. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption / password protection. If using my own device at home to view data, I will ensure that it is encrypted / password protected.
- I will use only school-provided portable storage (USB sticks, SD cards, portable hard drives etc) with encryption unless permission has been granted by the E-safety coordinator / Headteacher.
- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school. I will model safe and responsible behaviour in the creation and publishing of online content.
- I will use only school equipment to create digital images, video and sound unless prior permission is granted by the E-safety coordinator / Headteacher.
- I will ensure that I am familiar with the current permission status of pupils (see Parental Consent Form for Digital Images and Video). A summary of all permissions are circulated to all staff and available from the office. If additional permission is needed, e.g. for a surname in the press or for a medical form on SIMS, then I will discuss this with the E-safety coordinator and further written permission will be sought.
- I will ensure that I am familiar with the current Data Protection Policy. I will manage my digital files in accordance with this and I will make myself familiar with procedures in case of a breach of data security.
- I will not leave my computer unattended whilst working on screen; instead I will press CTL/ALT/DLT to lock the screen.
- I will only store / retain data files in line with the Data Retention Policy and will be responsible for deleting files which are no longer required.

School email and calendars

- I will use my school email address for all school-related correspondence. I understand that any use of the school email system will be monitored and checked. I will not use my private email account for any school-related business. Email is the main method of communication for all school matters and I will check my e-mail regularly and respond in a timely manner (in normal working hours) to communications that require my attention.

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Communication between staff or members of the wider school community should be professional and related to school matters only. Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect members of staff. All communications to parents and carers should be sent to the office email account for onward transmission. It is best practice when emailing parents and/or carers to add all intended recipients to the BCC address field. This ensures that parents' personal email addresses are not visible to others.
- To avoid the misrepresentation of others I will not make changes to someone else's e-mail and then pass it on without making it clear where changes have been made.
- I will take great care when forwarding messages to ensure that no confidential or sensitive material (e.g. other's email addresses) are attached
- The school calendar on Central Hosting is the central calendar for all school matters. I will check it regularly and take events into account when planning lessons and visits etc. I will add events and appointments to the diary dates as necessary. I will also regularly check the school website calendar.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach / model an age-appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour to pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.
- I will ensure that all online services and software that I use as part of my teaching are appropriate and are used in line with current guidance.
- I agree to adhere by the school's Prevent guidelines and action plan.

B: Personal equipment and services

Social media and messaging

- I will not talk about my professional role in any capacity when using personal social media. I will not use social media tools to communicate with current or former pupils under the age of 18 nor to communicate with parents in a professional capacity. I will be mindful of potential conflicts of interest where a parent or carer of a child at the school is also a personal friend. I will set and maintain my profile on social networking sites to maximum privacy. I will not access social networking sites for personal use during school hours.
- If I experience any derogatory, negative or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and bring this to the attention of the e-safety coordinator or Headteacher.
- Use of school equipment or e-mail accounts for personal financial gain, gambling, political purposes or advertising is forbidden. However, nothing in this paragraph is intended to restrict members of staff conducting any trade union or professional association using school computers or e-mail accounts, outside of teaching hours.

Personal mobile phones and other devices

- I will not bring my mobile into teaching spaces unless with the overt permission of the Headteacher. If permitted, I will ensure that my mobile phone and any other personally-owned device is switched off or switched to silent mode and out of sight during teaching hours and used only in emergencies.
- I will not contact any parents or pupils on my personally-owned device unless in an emergency. If a pupil or parent contacts me using my personal device I will inform the

Headteacher as soon as possible. On educational visits my personal mobile phone may be used to contact the school.

- I will not use any personally-owned mobile device to take images, video or sound recordings in school without the overt, written permission of the Headteacher.
- I will seek permission from the E-safety coordinator / Headteacher if I need to synchronise any school email account with a personally-owned device. If permission is granted then I will ensure that the device has the appropriate technical controls such as encryption / password protection.

Data Processors found to be in breach of these rules may face disciplinary action in line with the school's disciplinary procedures.

Full name (Please print): _____

Signed:_____

Date:_____

Appendix 2 – Acceptable Use for KS2

Petersfield Church of England Aided Primary School
Pupil KS2 Rules for Responsible Internet Use

These rules will keep me safe and help me to be fair to others.

- I will ask permission to go online.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- If I need to bring a phone to school, I will pass it to the office for safe keeping.
- If I use material that is the work of others in my work, I will state where I found the information.
- I will use a range of passwords, keep all passwords safe and never share accounts.

I have read and understand these rules and agree to them.

Child's name: _____ Child's signature: _____

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text onto any social media that could upset, offend, identify or threaten the safety of any member of the school community. I have read and agree to the E-safety and Data Protection policies.

Parent's signature: _____ Date: _____

The school accepts no responsibility for inappropriate use of the Internet outside school, even when children are researching a school-based subject. Please see the E-Safety information for parents on the website.

Appendix 3 – Acceptable Use for EYFS / KS1

Think before you click

S 

I will only use the Internet and email with an adult's permission.

A 

I will only click on icons and links when I know they are safe

F 

I will only send friendly and polite messages

E 

If I see something I don't like on a screen, I will always tell an adult

Child's name: _____ Child's signature: _____

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text onto any social media that could upset, offend, identify or threaten the safety of any member of the school community. I have read and agree to the E-safety and Data Protection policies.

Parent's signature: _____ Date: _____

The school accepts no responsibility for inappropriate use of the Internet outside school, even when children are researching a school-based subject. Please see the E-Safety information for parents on the website.

Appendix 4 – Subject Access Request Form

Petersfield Church of England Aided Primary School,
Hurdleditch Road,
Orwell, SG8 5QG

Re: subject access request

Dear Petersfield School Data Protection Officer,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*	Please provide me with:

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Your name

For office use only	
Date received	
Identify checked	
Date actioned	
Date request completed	