OLDFIELD SCHOOL

DATA PROTECTION AND INFORMATION SECURITY POLICY

Last Review:	April 2018
Committee:	SLT
Date Ratified:	23/04/2018
Next Review:	April 2020

This policy should be read in conjunction with the Data Protection Act 1998 (DPA), the General Data Protection Regulation (2016), the Education Student (Information) Regulations 2005, the School Staffing (England) Regulations 2009 (these apply to maintained schools), Independent School Standards Regulations 2010 (these apply to academies) and the ICO 'Report on the data protection guidance we gave schools 2012'. It also cross references and/or works in conjunction with other policies: Freedom of Information, ICT, E-Safety, Child Protection and Medical Conditions, and all policies related to recruitment of staff, complaints and disability.

1. Background

1.1. Data protection regulation applies only to living individuals.
1.2. There are stringent regulations that apply to the collection, using, disclosing, storing or disposing of personal data.
1.3. There are even stricter regulations that apply to what is termed 'special personal data'. This is information that relates to race, ethnicity, political opinions, religious beliefs, membership of trade unions, genetics, biometrics (where used for ID purposes), physical or mental health, and sex life or sexual orientation. Schools all hold a great deal of special personal data in their student and staff records.
1.4. In this context, the school (technically the governing body) is the data controller for the purposes of the relevant legislation and has the primary responsibility for ensuring that all legal requirements are met.
1.5. The school is legally obliged to protect any information, either personal data or special personal data, about students and staff from unauthorised access and from accidental loss or damage.
1.6. The school has a duty to notify the regulator for data protection regulation in this country - the Information Commissioner's Office (ICO) that we are processing personal data and therefore are data controllers. That notification must be renewed whenever the data held changes in any substantial way.
1.7. The school has a duty to inform data subjects regarding the personal data it processes on them – the school does this through its Privacy Notices.
1.8. Under data protection regulation, any individual has the right to make a request to access the personal information held about them.
1.9. In addition, under the school may hold some information about parents and carers.
1.10. The Education Student Information Regulations 2005 cover the rights of parents/carers to access their child's educational record.
1.11. There is a statutory exception to the above, where parents/carers do have an automatic right to access defined materials under the Education (School Records) Regulations 1989. The school will observe these statutory rights.

2. Introduction

2.1. In order to function properly we need to collect and use certain types of information about staff, students and other individuals who come into contact with the school. We are also obliged to collect and use data to fulfil our obligations to the local authority (LA), DFE and other bodies. We deal with information properly in whatever way it is collected, recorded and used – on paper, electronically or any other way. We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We are conscious that much of the data we hold is classified as special personal data and we are aware of the extra care this kind of information requires. We ensure that our organisation treats all personal information lawfully and correctly. To this end, we fully endorse and adhere to the data protection principles as contained in the General Data Protection Regulation

3. Data protection principles

3.1. All members of staff employed at Oldfield School are required to adhere to the eight enforceable data protection principles as set out in the General Data Protection Regulation

3.1.1. processed lawfully, fairly and in a transparent manner in relation to individuals;

3.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

3.1.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

3.1.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

3.1.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. School practice

4.1. Within school we strictly apply the following criteria and controls. These are to:

4.1.1. Notify the ICO that we process personal data and re-notify if procedures change or are amended.

4.1.2. Observe fully the conditions regarding the fair collection and use of information. To achieve this we have in place and use a privacy notice, sometimes called a fair processing notice – see Section 6.

4.1.3. Meet our legal obligations to specify the purposes for which information is used.

4.1.4. Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

4.1.5. Ensure the quality of information used.

4.1.6. Apply strict checks to determine the length of time information is held.

4.1.7. Ensure that the rights of the persons about whom information is held can be fully exercised under the legislation. These include the right to be informed that processing is being undertaken, the right to access to one's personal information, the right to prevent processing in certain circumstances and the right to rectify information which is inaccurate, and in certain circumstances the right to erasure where consent.

4.1.8. Take appropriate technical and organisational security measures to safeguard personal information. We will review the physical security of buildings and storage systems as well as access to them. All portable electronic devices must be kept as securely as possible on and off school premises.

4.1.9. Ensure that all Disclosure and Barring Service (DBS) records are kept in a safe central place and that no unnecessary certification information is kept longer than six months.

4.1.10. Ensure that personal information in not transferred outside of the European Economic Area without suitable safeguards.

4.1.11. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

4.1.12. Set out clear procedures for responding to requests for information – see Section 5.

4.1.13. Have in place secure methods for safely disposing of all electronic and paper records.

4.1.14. Be sure that photographs of students are not included in any school publication or on the school website without specific consent.

4.2. We shall also ensure that:

4.2.1. There is a named person with specific responsibility for data protection within the school.

4.2.2. All persons managing and handling personal information understand that they are contractually responsible for following good data protection practice.

4.2.3. All persons managing and handling personal information are trained to do so.

4.2.4. Anyone wanting to make enquiries about handling personal information knows what to do.

4.2.5. Anyone managing and handling personal information is appropriately supervised.

4.2.6. Queries about handling personal information are properly and courteously dealt with.

4.2.7. Methods of handling personal information are clearly described. Guidance for staff is detailed in Appendix A

4.2.8. A regular review and audit is made of the way personal information is held, managed and used.

4.2.9. Methods of handling personal information are regularly assessed and evaluated.

4.2.10. Performance with handling personal information is regularly assessed and evaluated.

4.2.11. A breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned.

4.2.12. Any breach of policy or regulation, including near misses are reported to the schools Data Protection Officer and are then investigated and reported to the ICO and affected data subjects (if there is high risk to their rights and freedoms).

4.2.13. On occasions when information is authorised for disposal, it is done appropriately.

4.2.14. Data protection risks are considered from the outset with any new process, product or service

4.2.15. High risk processing (special personal data) or use of CCTV will have a Data Protection Impact Assessment conducted.

5. Dealing with a subject access request (request for personal data)

5.1. Requests for information must be made in writing (which includes the use of e-mail) and be addressed to the headteacher. If the initial request does not clearly specify the information required, then the school will make further enquiries.

5.2. The headteacher must be confident of the identity of the individual making the request. When the request concerns data about a student, checks will also be carried out regarding proof of relationship to the child. In addition, evidence of identity will be established by requesting production of:

5.2.1. Passport.

5.2.2. Driving licence.

5.2.3. Utility bills with the current address.

5.2.4. Birth/marriage certificate.

5.2.5. P45/P60.
5.2.6. Credit card or mortgage statement (this list is not exhaustive).

5.3. As stated above, any individual has the right of access to information held about them. However, in the case of children this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. The headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility shall make the decision on behalf of the child.

5.4. The school may make a charge for the provision of additional copies, the school will not charge for the initial request, or if the requester simply wants to view the educational record of a child.

5.5. The response time for subject access requests, other than for educational records, is 30 days from receipt, this can be extended to 60 days if the request is complex

5.6. The regulation allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

5.7. Third party information is information that has been provided by another person such as the LA, the police, a health care professional or another school. It is normal good practice to seek the consent of the third party before disclosing information. Even if the third party does not consent, or consent is explicitly not given, the data may be disclosed. (There is no need in the case of third party requests to adhere to the 30-day statutory timescale).

5.8. Any information that could cause serious harm to the physical, emotional or mental health of a student or another person may not be disclosed, nor should information that would reveal that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.

5.9. If there are concerns about the disclosure of information, then additional advice should be sought, from our Data Protection Officer and potentially the Information Commission's Office.

5.10. When redaction (blacking out or obscuring of data) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

5.11. Information disclosed should be clear, with any codes, technical terms, abbreviations or acronyms explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.

5.12. Information can be provided at the school with a member of staff on hand to assist if requested, or provided at face-to-face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered or recorded mail will be used.

5.13. Complaints will be dealt with in accordance with the school complaints procedure, which is available on-line. Should the complainant wish to take the matter further, it should be firstly routed through the school's Data Protection Officer, and can then be escalated to the Information Commissioner www.ico.gov.uk.

6. Privacy Notice

6.1. Schools, LAs and the DFE all hold data on students in order to run the education system. In so doing, all have to follow the Data Protection Act 1998. The chief implication of this is that data held about students may only be used for specific purposes permitted by law. This notice is to inform you what types of data we hold, why it is held and to whom it may be passed on.

6.1.1. We hold information on students in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care and to help us assess how the school is performing overall. This data will include contact details, national curriculum assessment results, attendance information, characteristics such as ethnicity, SEN and any relevant medical information.

6.1.2. The school may include images of or information about students on the school website. If this is a problem to you for any reason, please let us know and we will ensure that this information is not included. However, parents/carers do need to know that at times we may be legally bound to disclose information to other bodies such as the police which the school will try to do with the knowledge of the relevant parents/carers.

6.1.3. From time-to-time, we are required to pass on information to the LA, DFE, to another school to which your child may be transferring, and other education related government bodies.

6.1.4. The government may require the school to share information with other agencies such as health, other LA departments and other relevant public bodies. The school will inform parents/carers when this type of processing occurs and seek consent where this is necessary.

7. Monitoring and Review

The school will monitor the impact of the policy using a range of methods and information including:

- Logs of reported incidents.
- Surveys/questionnaires of students, parents/carers and staff.
- Audit, inspection and compliance reviews.
- Changes to the relevant legislation.

The policy will be reviewed in the light of any incidents that have taken place or significant new developments in the use of data storage and access technologies which may require a change to the policy, or perceived new threats related to online storage.

Appendix A – Data Handling Procedures

I understand that:

1. I will take care when **opening emails**, and that I will not assume that email is a trusted means of communication, including:
    1.1. Not opening links or attachments which I am not expecting – instead I will verify the validity of the email by other trusted means (e.g. phone call, SMS)
2. I will take care when **sending emails** by taking measures to ensure the email address is accurate
3. I will take measures to secure **personal data within external emails** by
    3.1. Encrypting the contents within a file or folder (password protected), ensuring the password is shared using a different communication method (e.g. phone call, SMS)
    3.2. Using anonymisation or pseudonymisation (using a unique identifier which only the sender/recipient can match up to a name)
4. I will take measures to secure **hardcopy documents** by
    4.1. Ensuring I double check any postal addresses where personal data or special personal data is posted out
    4.2. Ensuring I send the package via recorded delivery for any special personal data where other secure means are not available.
    4.3. Disposing of them either through a cross shredder or through the schools confidential waste provider.
5. Ensure **clear desk / clear screen** principles are maintained, by
    5.1. Clearing away documents containing any personal or special data when I am away from my desk for a short period
    5.2. Locking away personal data when I am away from my desk for an extended period (e.g. packing up for the day)
    5.3. Locking my screen when I am away from my device using ⊞ + L
6. I will ensure personal data is not removed from the school site by:
    6.1 Only storing electronic personal data (e.g. electronic markbooks, assessment data with student names) on the school server, and not saving this in any removable device (such as a memory stick).
    6.2 Only accessing data securely at home through remote access, not using public networks or computers. Ensuring that remote access connection is terminated immediately after use.