PROSPER
LEARNING TRUST

Data Protection Policy

DOCUMENT HISTORY

Policy reviewed and adopted by Trustees	**December 2017**
Reviewed	**November 2018**
Review frequency	**Annually**
Date of next review	**October 2019**
Responsible Officer	**Data Protection Officer**

Data Protection Policy

This document is a statement of the aims and principles of the Prosper Learning Trust, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents/carers and governors.
This policy should be implemented within the context of the vision, aims and values of each of our academies.

1. Introduction

Prosper Learning Trust and its academies need to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. 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, Prosper Learning Trust must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 and GDPR 2018.

In summary these state that personal data shall be:

- obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- adequate, relevant and not excessive for that purpose
- accurate and where necessary, kept up to date
- not kept for longer than is necessary for that purpose
- processed in accordance with the data subject's rights
- kept safe and secure, from unauthorised access, accidental loss or destruction
- not transferred outside of the European Economic Area

(Appendix 1 defines some of these statements further)

Prosper Learning Trust and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Trust has developed this Data Protection Policy.

2. Status of this 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 Trust. Any failures to follow the policy can therefore result in disciplinary proceedings.

3. The Data Controller and the Designated Data Controllers

Prosper Learning Trust as a body corporate is the Data Controller, and the Board of Trustees are therefore ultimately responsible for the implementation of the Data Protection Policy.

Prosper Learning Trust has appointed a designated Data Protection Officer who deals with day to day matters, is the named person in the notification to the Data Protection Commissioner and oversees implementation of new regulations brought about by GDPR.

4. Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide, in connection with their employment is accurate and up to date
- Informing the relevant academy of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The academy cannot be held responsible for any errors unless the staff member has informed the academy of such changes
- Attending all Data Protection Training offered and implementing any changes needed into their working procedures

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines from Data Protection Training and this and other relevant policies.

5. Data Security

Prosper Learning Trust undertakes to ensure security of personal data by the following general methods:

- **Physical security**

Personal information is kept in a locked filing cabinet, drawer or safe. Only authorised persons are allowed in the offices. Offices are locked when not in use. Visitors are required to sign in and out, to wear identification badges whilst in the academy and are, where appropriate, accompanied.

- **Logical security**

Computerised data is coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on any removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken.

- **Procedural security**

In order to be given authorised access to the computer, staff will have to undergo enhanced DBS checks and will be made aware of the relevant policies. Computer printouts as well as source documents are shredded before disposal.

All staff are made aware of their Data Protection obligations.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

6. Rights to Access Information

All staff, students, parents and other users are entitled to:

- Know what information the Trust and its constituent academies hold and process about them or their child and why
    - The Trust will publish Privacy Notices (Appendix 3) on their website and display boards, informing all staff and parents and other relevant users, the personal data held about them. This will state all the types of data the Trust holds and processes about them, and the reasons for which they are processed.

- Know how to gain access to it
    - All staff, students, parents and other users have a right to access certain personal data being kept about them or their child either on computer or in files. Any person who wishes to exercise this right should make a written request or complete the Subject Access Request Form (Appendix 2 – available on website) and submit it to the Data Protection Officer (Where a request for subject access is received from a student, it will be processed as any subject access request and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request, when it will be referred to their parents or carers.)
    - The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days in order to adhere to GDPR
    - Where a Subject Access Request (SAR) is made for information containing in whole or in part, a pupil's "education record", a response must be provided in 15 days and there will be no charge

- Know how to keep it accurate and up to date
    - Updates of staff and student data will be requested yearly in order to ensure data is kept up to date
    - Parents/carers are requested to inform their academy's office if their contact details change

- Know what the Prosper Learning Trust is doing to comply with its obligations under the Data Protection Acts
  - This Policy and the Privacy Notices are available on the Trust's website to inform all parties
  - Training will be provided regularly for all staff to ensure an understanding of responsibilities of Data Protection and new regulations as they are adopted
- Request that some data is erased or processing is restricted (especially in relation to automated processes)
- Request that data is transferred when required
- Object to the processing of their data

7. Subject Consent

In many cases, the Trust can only process personal data with the consent of the individual. In some cases, if the data is Special Category Data, as defined in the Data Protection Acts, consent must be obtained unless specific reasons are fulfilled.

Consent must be:

- Freely given, specific, informed and unambiguous indication of the subject's wishes
- Clear, affirmative action (a positive OPT-IN)
- Cannot be inferred from silence or inactivity
- Consent must be separate from other terms and conditions
- Must be as simple to withdraw as it was to give
- Brings additional rights to the data subjects
- Must be verifiable

Prosper Learning Trust has consent forms which conform to GDPR for photography and biometric information. If any other information is processed which requires consent the relevant forms will be designed.

8. Special Category Data

All posts within Prosper Learning Trust will bring the applicants into contact with children. The Trust and its constituent academies has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and has a duty of care to all staff and students, so must therefore make sure that employees and those who use academy facilities do not pose a threat or danger to other users. The Trust may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. This information will only be used in the protection of the health and safety of the individual.

When it is necessary to process Special Category Information, this may be to ensure that the academy is a safe place for everyone, or to operate other policies, such as the Sick Pay Policy or the Equal Opportunities Policy.

Prosper Learning Trust will only process this data if:

- It is required by employment, social security or social protection law
- It is necessary to protect the vital interests of a Data Subject
- It is necessary for reasons of substantial public interest
- It is necessary for archiving purposes in the public interest
- Explicit consent has been given

9. Publication of Academy Information

Certain items of information relating to Prosper Learning Trust staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with The Trust or its constituent academies.

10. Retention of Data

Prosper Learning Trust has a duty to retain some staff and student personal data for a period of time following their departure from the academy, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time in accordance with the Information Management Toolkit for Schools from the Information and Records Management Society, www.irms.org.uk

11. Enquiries or Complaints

The Data Protection Policy is available from the Trust website or Academy offices.

General information about the Data Protection Act can be obtained from the Information Commissioner's Office **0303 123 1113**, website www.ico.gov.uk.

Any member of staff, parent/carer or other individual who considers that the Policy has not been followed in respect of personal data about themselves or their child should raise the matter with the Data Protection Officer, Victoria Hall, on 0191 9171246 or Victoria.hall@properlearningtrust.co.uk.

Appendix 1

Fair obtaining and processing

We will inform all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

- "processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data
- "data subject" means an individual who is the subject of personal data or the person to whom the information relates
- "personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media
- "parent" has the meaning given in the Education act 1996 and includes any person having parental responsibility or care of a child

Registered purposes

The Data Protection Registration entries for the Trust are available for inspection, by appointment, at the Academies' offices or from the ICO website www.ico.org.uk. Explanation of any codes and categories entered is available from the Data Protection Officer. Registered purposes covering the data held are listed on the Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Appendix 2

Subject Access Request Form

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the Trust/Academy holds about them, and can make a Subject Access Request (SAR). A SAR can be made using the 'Subject Access Request' form, below.

The DPO has been designated as the person who will coordinate the response to a SAR. The school is required to provide the individual with the data it holds on them within 30 days.

The response to the SAR will be provided in an electronic form unless specifically requested otherwise. It is permissible to ask the individual who has made the request to be more specific about the information that they require in order to ensure that the information they are provided with meets their requirements rather than providing lots of information that may not be relevant to their query.

Evidence of the identity of the person making the request and their relationship to the pupil must be gained prior to any disclosure of information. This will be recorded on the SAR Log.

Data Subjects Details (person whose information you are requesting)

Title:	
Full Name:	
Date of Birth:	
Address:	
Year Group (if pupil)	

Requestor Details

Title:	
Full Name:	
Address:	
Phone Number:	
Email Address:	
Evidence of Identity:	Passport/Driver's License etc: Signed by authorised person :
Status of requestor:	Data Subject: Yes/No Parent or person with Parental Responsibility: Yes/No Other: (Please outline role)

Details of Subject Access Request

Details of Data Being Requested	

Declaration
Please complete the statement which applies to you.

I, _____, hereby request that Prosper Learning Trust provide the data requested about me.

Signed: _____ Date:_____

Or

I, _____, hereby request that Prosper Learning Trust provides the data requested about _____(insert dependants's name) on the basis of the authority that I have as parent/carer.

Signed: _____ Date:_____

Please return this completed form to Victoria.Hall@prosperlearningtrust.co.uk

Appendix 3

Privacy Notice
How We Use Pupil Information

Under data protection law, individuals have a right to be informed about how PROSPER Learning Trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about pupils who attend any of the academies in out trust.

We, Prosper Learning Trust, are the 'data controller' for the purposes of data protection law.

The categories of pupil information that we collect, process, hold and share:

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents (to confirm name, unique pupil number, address, age etc.)
- Characteristics (such as ethnicity, language, nationality, country of birth, SEND information and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Safeguarding information (including involvement of other agencies such as court orders and professional involvement)
- Details of any medical conditions, including physical and mental health (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- Results of internal assessments and externally set tests/exams and post 16 courses enrolled for
- Pupil and curricular records (including previous schools' information)
- Behavioural information (exclusions/reports)
- Details of any support received, including care packages, plans and support providers
- Biometric information for school meal management
- Photographs or video
- CCTV images captured in schools
- Educational Visit information (including permissions, emergency contacts, visit reports etc.)

This list is not exhaustive - we may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education. The data asset register and updated privacy notices will be made available on the PROSPER Learning Trust website which is currently in production.

Why we collect and use this information

We collect and use the pupil data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil's welfare
- Keep children safe (medical conditions, food allergies, or emergency contacts)
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
- To meet the statutory duties placed upon us for DfE data collections

The lawful basis on which we process this information

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' special category data in situations where:

- We have obtained explicit consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)
- Processing is necessary for reasons of substantial public interest

Where we have obtained consent to use pupil's personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting pupil information

We collect pupil information via registration forms at the start of the school year/on entry to the school or Common Transfer File (CTF) or secure file transfer from any previous school.

Pupil data is essential for the schools' operational use. Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the data protection legislation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing this information

We keep personal information about pupils while they are attending schools within the Trust. We may also keep it beyond their attendance at these schools if this is necessary in order to comply with our legal obligations. Our data retention schedule sets out how long we keep information about pupils. A copy of this schedule is available upon request from the Trust office. Pupil information will be held on personal file and on the Trust's Management Information System – SIMS.

The trust is committed to keeping the personal data that it holds safe from loss, corruption or theft. The measures in place to do this include:

- Data protection training for all employees local governors and directors/trustees
- Policies and procedures detailing what employees and office holders can and cannot do with personal data
- Various IT security safeguards such as firewalls, encryption, and anti-virus software
- On-site security safeguards to protect physical files and electronic equipment

For the purpose of community teaching/school outings a list of (emergency) contacts will be taken off school premises and held securely by the lead teacher in each case.

Who we share pupil information with

We routinely share pupil information with:

- Schools that the pupils attend after leaving us
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns, exclusions and attendance
- The Department for Education – see below
- Pupil's family and representatives
- Examining bodies
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Our regulator – Ofsted
- Police forces, courts, tribunals
- Professional bodies
- Health and social welfare organisations
- Professional advisers and consultants
- Health authorities
- Central and local government
- Connexions (careers service)/youth support services (pupils aged 13+)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013. This data sharing underpins school funding and educational attainment policy and monitoring.

In order to deliver the best possible education PROSPER Learning Trust often uses other service providers. These organisations will sometimes require access to your personal data in order to complete their work. If the trust does use a third party organisation it will always have an agreement in place to ensure that the other organisation keeps your data secure and only uses it for the agreed purpose(s).

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education, go to:
https://www.gov.uk/education/data-collection-and-censuses-for-schools

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996

This enables them to provide services as follows:

- Youth support services
- Careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the pupil once they reach the age of 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996

This enables them to provide services as follows:

- Post-16 education and training providers
- Youth support services
- Careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils)(England) Regulations 2013.

To find out more about the NPD, go to
https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

The Department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis
- Producing statistics
- Proving information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decision on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data
- The purpose for which it is required
- The level and sensitivity of data requested: and
- The arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the Department's NPD data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisation the department has provided pupil information, (and for which project), please visit the following website:

https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them **(Subject Access Request)** that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Victoria Hall, Data Protection Officer.

If you make a Subject Access Request, and if we do hold information about you or your child we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decision being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations either through the ICO, or through the courts

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about out data processing, please raise this with us in the first instance.

To make a complaint please contact Victoria Hall, Data Protection Officer (see contact details below).

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Further information

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact Victoria Hall, Data Protection Officer at admin@prosperlearningtrust.co.uk

Privacy Notice
How We Use School Workforce Information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, PROSPER Learning Trust, are the 'data controller' for the purposes of data protection law.

The categories of school workforce information that we collect, process, hold and share

We process data relating to those we employ, or otherwise engage to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Personal information (such as name, addresses, date of birth, employee or teacher number, national insurance number, and next of kin/emergency contact details)
- Salary, annual leave, payroll records - payroll number, bank account details, tax status information, pension and benefits information
- Contract information (such as start dates, hours worked, positions held)
- Recruitment information, including copies of right to work documentation, references and other information included in the application form/letter or as part of the application process
- Qualifications and employment records, including work history, job titles, training records and professional memberships (and, where relevant, subjects taught)
- Work absence information (such as number of absences and reasons)
- Performance information
- Relevant medical information
- Outcomes of any disciplinary and/or grievance procedures
- Copy of driving licence, (if necessary)
- Photographs
- CCTV footage
- Data about your use of the school's information and communications systems

This list is not exhaustive, an up to date Data Asset Register and relevant updated privacy notices will be available on the Prosper Learning Trust website (currently in construction).

Why we collect and use this information

We use school workforce data to help us run the school, including to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid, with correct taxes and pensions arrangements
- Keep employees safe and enable wellbeing
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Allow better financial modelling and planning
- Supporting the work of the School Teachers' Review Body and other governmental staff review bodies
- Complete the school workforce census (must be completed by law)

The lawful basis on which we process this information

We only collect and use personal information about you when the law allows us to. Under the General Data Protection Regulation (GDPR), the legal bases we rely on for processing personal information for general purposes are to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- Processing is necessary for carrying out obligations under employment, social security or social protection law

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

Workforce data is essential for the school's operational use. Whilst the majority of information you provide to us is mandatory, (e.g. through application/contract forms) some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Information will also be on school's management information system (SIMS).

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our data retention schedule, which will be available on PROSPER Learning Trust website.

Who we share this information with

We routinely share this information with:

- The Local Authority
- The Department for Education (DfE)
- Pensions and tax organisations (Teachers' Pensions, Tyne and Wear Pensions Fund, HMRC)

We may, if necessary also share some information with:

- Educational IT systems
- OFSTED
- Our auditors
- Health authorities
- Educators and examining bodies
- Professional bodies
- Charities and voluntary organisations
- Police forces, courts, tribunals

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so. Where it is legally required or necessary (and it complies with data protection law) we may share personal information about you with

Local authority – we are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. It is also shared for payroll purposes while the LA act as the school's payroll provider.

Department for Education (DfE) – we share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment of educational attainment.

We are required to share information about our school employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to
https://www.gov.uk/education/data-collection-and-censuses-for-schools

Transferring data internationally

We will avoid transferring personal data to a country or territory outside the European Economic Area, in order to comply with data protection law. Where this is unavoidable it will **only** be, when necessary, for important reasons of public interest and where adequate safeguards are in place.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold ('subject access request'). To make a written request for your personal information, contact Victoria Hall, Data Protection Officer for a Subject Access Request Form.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy in an intelligible form

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decision being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations either through the ICO, or through the courts

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint please contact Victoria Hall, Data Protection Officer (see Further Information below).

Alternatively, you can contact the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns
- Call 0303 123 1113
- Or write to: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

If you would like to discuss anything in this privacy notice, please contact Victoria Hall, Data Protection Officer, at: Victoria.Hall@ProsperLearningTrust.co.uk or 0191 9171246.

Appendix 4

Clear Screen and Desk Policy

Introduction

Information is an asset. Like any other business asset it has a value and must be protected. Systems that enable us to store, process and communicate information must also be protected in order to safeguard information assets. 'Information systems' is the collective term for our information (both paper-based and computerised) and the systems we use to store, process and communicate it.

This document should be read in conjunction with other information system policies and procedures all of which are published on the Trust's website:

- Data Protection Policy
- Freedom of Information Policy
- Privacy Notices
- Complaints Policy
- E-Safety Policy

Rationale

PROSPER Learning Trust (PLT) holds information about pupils, parents and staff in both computerised and paper forms, including particularly sensitive Special Category Data (health reports, SEN, child protection etc) . The Trust is at risk of a serious data breach of unauthorised access to electronic records, when unlocked PC screens are left unattended or when paper records are left on desks/workstations overnight or for long periods of time. Both are at risk of theft, unauthorised disclosure and damage.

Clear desks and clear screens protect against a data breach and also ensure that the Trust projects a professional and efficient image to visitors, members of the public and colleagues.

Roles and Responsibilities

It is important that all staff understand what is required of them and comply with this policy.

All staff are responsible for ensuring the information on their desk/workstation or screen is adequately protected in compliance with all relevant school policies and procedures.

Line Managers have a responsibility to ensure their staff are following procedures.

The Data Protection Officer has the responsibility to advise the Trust on data protection legal obligations and procedures to keep data safe, and to monitor compliance across the trust.

Scope

This policy applies to everyone who has access to the PLT's information, information assets or IT equipment. This may include, but is not limited to employees of the PLT, trustees and governors, temporary workers, partners and contractual third parties.

All those who use or have access to information must understand and adopt this policy and are responsible for ensuring the security of the Trust's information systems and the information that they use or handle.

This policy sets out PLT's requirements for each member of staff to protect any documents or records which are kept at their desk/workstation either temporarily or permanently and covers records in all formats including:

- Paper
- Electronic documents
- Emails
- Visual images such as work related photographs
- Audio and video CDs, DVDs etc
- Memory sticks and portable hard drives
- Databases

Clear Desk Procedure

All personal information about pupils, parents or staff **must** be locked away when not in use and never left unattended. Ideally, all staff should leave their desk paper free at the end of the day.

Ensure that you select an appropriately located printer where you are able to retrieve your printing immediately. Do not leave personal information for others to find. Coded printing will be used where possible when appropriate.

An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible **– "Do you need to print it"?**

Ensure documents are disposed of securely. Never put documents containing personal or corporate sensitive information in the general waste bins. Use the confidential paper shredding boxes.

All Portable Computing & Data Storage Devices (PCDs) such as USB data sticks, mobile phones and laptops should be locked away at the end of the working day.

Clear Screen Procedure

Always lock the desktop when leaving the workstation/desk unattended. If using a shared workstation/desk log off rather than lock it. If anticipating an absence of more than 30 minutes log off or shutdown the computer. This also applies when using a laptop.

Pressing CTRL+ALT+DEL and clicking 'Lock this computer' is straight forward and simple. However, a windows key combination is even simpler. Press windows key + L and your computer will lock automatically. (The windows key can usually be found in the bottom left of the keyboard and looks like a flag/window.)

To unlock press CTRL+ALT+DEL and log back in.

Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorised people while in use.

Always shutdown all computers at the end of every day!!

Monitoring Procedure

Line Managers should make random spot checks throughout the year, on unattended desks/screens, particularly when rooms are empty and at the end of the day.

Please document on the Monitoring Form below and return to the Data Protection Officer at the end of each school year.

Clear Screen and Desk Monitoring Form

Line Manager:

Date	Name	Clear Desk	Clear Screen	Action Taken