Data Protection Policy

Ref: A02

Content:

Document Control	
Title	A02: Data Protection Policy
Date	September 2023
Supersedes	Previous Trust Data Protection Policy
Amendments	Revised with up to date guidance from Judicium
Related Policies/Guidance	Cyber Security Policy Data Breach Policy Data Protection Policy Data Retention Policy Freedom of Information Policy ICT Acceptable Use Policy Subject Access Request Policy
Review	Every 1 Year
Author	A. Bryan / Judicium
Date consultation completed	N/A
Approved Level:	Chief Executive Officer
Date adopted:	1st September 2023
Expires on	31st August 2024

Prospere Learning Trust
is a Multi Academy Trust
Registered in England and Wales number 10872612
Registered Office: Firbank Road, Manchester, M23 2YS

The Prospere Learning Trust has several Trust-wide policies which are adopted by all schools/academies in the Trust to ensure an equitable and consistent delivery of provision.

The Trust Board has responsibility for the operational of all schools/academies and the outcomes of all students however responsibility is delegated to the Local Governing Body of each school via the Scheme of Delegation.

Within our policies reference to:

- Governing Body / Governors relates to the members of the Local Governing Body representing the Trust Board.
- School includes a reference to school, academy or free school unless otherwise stated.
- Headteacher includes a reference to Headteacher, Principal or Head of School of a school, academy, or free school.

1. SECTION 1 – INTRODUCTION & DEFINITIONS

1.1. The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

1.2. The Trust will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

1.3. This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

1.4. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

1.5. Personal data: Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

1.6. Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

1.7. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

1.8. Special Category Data: Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

1.9. Data Subject: An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

1.10. Data Controller: The organisation storing and controlling such information, Prospere Learning Trust is referred to as the Data Controller.

1.11. Processing: Processing data involves any activity that involves the use of personal data. This includes but is not limited to obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

1.12. **Automated Processing:** Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

1.13. An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

1.14. **Data Protection Impact Assessment (DPIA):** DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

1.15. **Criminal Records Information:** This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

2. SECTION 2 - WHEN CAN THE TRUST PROCESS PERSONAL DATA

2.1. Data Protection Principles: The Trust are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR.

2.2. The principles the Trust must adhere to are set out below.

2.3. Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner. The Trust only collects, processes and shares personal data fairly and lawfully and for a specified purposes. The Trust must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

2.4. Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

2.5. Personal Data: The Trust may only process a data subject's personal data if one of the following fair processing conditions are met: -

a) The data subject has given their consent;

b) The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;

c) To protect the data subject's vital interests;

d) To meet our legal compliance obligations (other than a contractual obligation);

e) To perform a task in the public interest or in order to carry out official functions as authorised by law;

f) For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

2.6. Special Category Data: The Trust may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met:

a) The data subject has given their explicit consent;

b) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;

c) To protect the data subject's vital interests;

d) To meet our legal compliance obligations (other than a contractual obligation);

e) Where the data has been made public by the data subject;

f) To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;

g) Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

h) Where it is necessary for reasons of public interest in the area of public health;

i) The processing in necessary for archiving, statistical or research purposes.

2.7. The Trust identifies and documents the legal grounds being relied upon for each processing activity.

2.8. Consent: Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

2.9. Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

2.10. A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

2.11. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

2.12. If explicit consent is required, the Trust will normally seek another legal basis to process that data. However, if explicit consent is require the data subject will be provided with full information in order to provide explicit consent.

2.13. The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

2.14. **<u>Principle 2:</u> Personal data must be collected only for specified, explicit and legitimate purposes.** Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

2.15. The Trust will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

2.16. **<u>Principle 3:</u> Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.** The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

2.17. When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data.

2.18. **<u>Principle 4:</u> Personal data must be accurate and, where necessary, kept up to date.** The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

2.19. Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

2.20. **<u>Principle 5:</u> Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.** Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data.

2.21. We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

2.22. Please refer to the Trust's Retention Policy for further details about how the Trust retains and removes data.

2.23. **<u>Principle 6:</u> Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage**

2.24. In order to assure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

a) Encryption;

b) Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);

c) Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);

d) Adhering to confidentiality principles;

e) Ensuring personal data is accurate and suitable for the process for which it is processed.

2.25. The Trust follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

2.26. The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

2.27. Sharing Personal Data: The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

a) Has a need to know the information for the purposes of providing the contracted services;

b) Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;

c) The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

d) The transfer complies with any applicable cross border transfer restrictions; and

e) A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

2.28. There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

2.29. The intention to share data relating to individuals to an organisation outside of our Trust shall be clearly defined within written notifications and details and basis for sharing that data given.

2.30. Transfer of Data Outside the European Economic Area (EEA). The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

2.31. The Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

2.32. Transfer of Data Outside the UK. The Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct**.**

3. SECTION 3 - DATA SUBJECTS' RIGHTS AND REQUESTS

3.1. Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

3.2. The rights data subjects have in relation to how the Trust handle their personal data are set out below: -

a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

b) Receive certain information about the Trust's processing activities;

c) Request access to their personal data that we hold (see Subject Access Requests Policy);

d) Prevent our use of their personal data for marketing purposes;

e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

f) Restrict processing in specific circumstances;

g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

i) Object to decisions based solely on automated processing;

j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

l) Make a complaint to the supervisory authority; and

m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

3.3. If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request.

3.4. Direct Marketing: The Trust are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

3.5. The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

3.6. Employee Obligations: Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, you must: -

a) Only access the personal data that you have authority to access, and only for authorised purposes;

b) Only allow others to access personal data if they have appropriate authorisation;

c) Keep personal data secure (for example by complying with rules on access to Trust premises, computer access, password protection and secure file storage and destruction (Please refer to the Trust's Security Policy for further details about our security processes);

d) Not to remove personal data or devices containing personal data from Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;

e) Not to store personal information on local drives.

4. SECTION 4 - ACCOUNTABILITY

4.1. The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

4.2. The Trust have taken the following steps to ensure and document UK GDPR compliance: -

a) **Data Protection Officer (DPO):** Please find below details of the Trust's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

4.3. The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

4.4. Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

a) If you are unsure of the lawful basis being relied on by the Trust to process personal data;

b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

c) If you need to draft privacy notices or fair processing notices;

d) If you are unsure about the retention periods for the personal data being processed (refer to the Trust's data retention policy in the first instance;

e) If you are unsure about what security measures need to be put in place to protect personal data;

f) If there has been a personal data breach (see Data Breach Policy for further information);

g) If you are unsure on what basis to transfer personal data outside the EEA;

h) If you need any assistance dealing with any rights invoked by a data subject;

i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

j) If you plan to undertake any activities involving automated processing or automated decision making;

k) If you need help complying with applicable law when carrying out direct marketing activities;

l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

4.5. Personal Data Breaches: The UK GDPR requires the Trust to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

4.6. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

4.7. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches who is the Headteacher (or IT Infrastructure Director for cyber incidents or your DPO.

4.8. Transparency and Privacy Notices: The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the Trust use their data and the Trust's privacy notices are tailored to suit the data subject.

4.9. Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the Trust's contact details, how and

why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

4.10. When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The Trust will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

4.11. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the UK GDPR

4.12. Privacy By Design: The Trust adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

4.13. Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

4.14. Data Protection Impact Assessments (DPIAs): In order to achieve a privacy by design approach, the Trust conduct DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event the Trust carries out DPIAs when required by the UK GDPR in the following circumstances: -

a) For the use of new technologies (programs, systems or processes) or changing technologies;
b) For the use of automated processing;
c) For large scale processing of special category data;

d) For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

4.15. Our DPIAs contain: -

a) A description of the processing, its purposes and any legitimate interests used;
b) An assessment of the necessity and proportionality of the processing in relation to its purpose;
c) An assessment of the risk to individuals; and
d) The risk mitigation measures in place and demonstration of compliance.

4.16. Record Keeping: The Trust are required to keep full and accurate records of our data processing activities. These records include: -

a) The name and contact details of the Trust;
b) The name and contact details of the Data Protection Officer;
c) Descriptions of the types of personal data used;
d) Description of the data subjects;
e) Details of the Trust's processing activities and purposes;
f) Details of any third party recipients of the personal data;
g) Where personal data is stored;
h) Retention periods; and
i) Security measures in place.

4.17. Training: The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

4.18. **Audit:** The Trust regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

5. SECTION 5: STAFF RESPONSIBILITY for INFORMATION SECURITY

5.1. The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

5.2. The Trust is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the Trust **and the responsibilities of all staff** to achieve this, including to:

a) protect against potential breaches of confidentiality;

b) ensure that all information assets and IT facilities are protected against damage, loss or misuse;

c) uphold our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and

d) increase awareness and understanding throughout the Trust of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

5.3. Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

5.4. For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

5.5. **Scope:**

a) The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Trust, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

b) This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

c) All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy up to and including summary dismissal depending on the seriousness of the breach.

d) This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

5.6. **General principles:**

a) All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information.) All data so classified must be handled appropriately in accordance with its classification.

b) Staff should discuss with Trust IT Team the appropriate security arrangements for the type of information they access in the course of their work.

c) All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

d) All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the Trust IT Team or by such third party/parties as the IT Infrastructure Director may authorise.

e) The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with IT Infrastructure Director unless expressly stated otherwise.

f) All staff have an obligation to report actual and potential data protection compliance failures to Andi Bryan – Trust GDPR Lead who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer.

5.7. Physical security and procedures:

a) All staff must ensure they follow the **Prospere Learning Trust 'Clear Workspace Protocol'** when handling personal data – See Appendix B.

b) Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g., through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

c) Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use.

d) Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

e) The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Headteacher as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

f) All Trust School's carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

g) Each School has an intercom system to minimise the risk of unauthorised people from entering the school premises.

h) All Schools close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

i) CCTV Cameras are in use at Schools across the Trust.

j) Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

5.8. Responsibilities of the Head of IT Services:

5.9. The Head of IT Services, shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Trust's security requirements;

b) ensuring that IT Security standards within the Trust are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;

c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990.

5.10. Furthermore, the Head of IT Services shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy;

b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;

c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;

d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];

e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;

f) monitoring all IT security within the Trust and taking all necessary action to implement this policy and any changes made to this policy in the future; and

g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

5.11. Responsibilities – ALL Members of staff:

a) All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

b) Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

c) You must immediately inform the Headteacher/ Head of IT Services of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

d) Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the IT helpdesk immediately.

e) You are not entitled to install any software of your own without the approval of the Headteacher / Head of IT Services. Any software belonging to you must be approved by the Headteacher / Head of IT Services and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

f) Prior to installation of any software onto the IT Systems, you must obtain written permission by the Headteacher / Head of IT Services. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

g) Usage of physical media (e.g., USB memory sticks or disk storage of any kind) for transferring files is not permitted. In exceptional circumstances permission to use physical media for storage MUST be obtained from the Headteacher prior to transferring files.

h) If you detect any virus this must be reported immediately to the IT Helpdesk (this rule shall apply even where the anti-virus software automatically fixes the problem).

5.12. Access security:

a) All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

b) The Trust has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Trust's network. The school's also teach individuals about e-safety / cyber security to ensure everyone is aware of how to protect the Trust's network and themselves.

c) All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

d) All passwords must, comply with the Trust's password protocols (See Appendix A).

e) Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Head of IT Services as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the Trust's Disciplinary Policy and Procedure.

f) Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

g) If you forget your password you should notify the IT Helpdesk to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

h) You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

i) Computers and other electronical devices with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

j) All mobile devices provided by the Trust, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

k) Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

5.13. **Data security**:

a) Personal data sent over the Trust network will be encrypted or otherwise secured.

b) All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from Head of IT Services who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems.

c) You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the School's WIFI access requirements and instructions governing this use. All usage of your own device(s) whilst connected to the Trust's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The Headteacher may at any time request the immediate disconnection of any such devices without notice.

5.14. Electronic storage of data:

a) All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the Head of IT Services.

b) All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

c) You should not store any personal data on any mobile device, whether such device belongs to the Trust or otherwise without prior written approval of the Headteacher. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the Trust's computer network in order for it to be backed up.

d) All electronic data must be securely backed up by the end of the each working day and is done by IT Services.

5.15. Home working:

a) You should not take confidential or other information home without prior permission of the Headteacher, and only do so where satisfied appropriate technical and practical measures

are in place within your home to maintain the continued security and confidentiality of that information.

b) When you have been given permission to take confidential or other information home, you must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

5.16. Communications, transfer, internet and email use:

a) When using the Trust's IT Systems you are subject to and must comply with the Trust's Acceptable Use of ICT Policy.

b) The Trust work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

c) If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to a member of SLT immediately.

d) Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the Trust cannot accept liability for the material accessed or its consequence.

e) All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

f) Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

g) You should be careful about maintaining confidentiality when speaking in public places.

h) You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Trust.

i) Personal or confidential information should not be removed from the Trust without prior permission from the Headteacher except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

5.17. Reporting security breaches:

a) All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Headteacher / Member of SLT. All members of staff have an obligation to report actual or potential data protection compliance failures.

b) When receiving a question or notification of a breach, the Headteacher / SLT shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue, liaising with the DPO for guidance.

c) Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Head of IT Services. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Headteacher.

d) Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Headteacher.

e) All IT security breaches shall be fully documented.

6. SECTION 6: MONITORING and REVIEW

6.1. Related Policies: Staff should refer to the following policies that are related to this data protection policy: -

a) Data Retention Policy

b) Subject Access Request Policy

c) Freedom of Information Policy

d) Data Breach Policy

e) Acceptable Use of ICT Policy

6.2. These policies are also designed to protect personal data and can be found on the Trust's EVERY management system.

6.3. Monitoring: We will monitor the effectiveness of this and all our policies and procedures and conduct a full review and update as appropriate.

6.4. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.

APPENDIX A: Prospere Learning Trust Password Policy

1. Overview:

1.1. Passwords are a key element of the Trusts IT security. Poorly chosen or weak passwords may result in the compromise of systems within the Trust network. As such, all Trust users (staff and students) are responsible for taking appropriate steps to securing and using their passwords.

1.2. Given the nature of the Trust and its cohort of students, there are variable requirements for passwords that differ between mainstream and special schools – these are detailed further in the document.

2. Password Guidelines:

2.1. The following guidelines should be followed by all users to ensure the security and integrity of their accounts.

a) Passwords must never be divulged or shared with anyone else.

b) Passwords must never be written down .

c) Users must never leave themselves logged in to any PC or system where someone else could unknowingly use their account.

d) Passwords should be unique and different from passwords used for other non-Trust services.

e) Passwords must be the designated minimum requirements outlined further in this policy.

2.2. In the event a breach or compromise is suspected, the incident must be reported to IT Services immediately.

2.3. Access to Office 365 and Remote Access when off-site must utilise MFA for all staff.

3. <u>Password Requirements:</u>

3.1. All password requirements are enforced via fine grained password policies within Active Directory IT Services Administrative Accounts

3.2. The password requirements for **IT Services Administrative Accounts** is:

a) Minimum Password Length: 12

b) Password History: 10

c) Lockout Policy:

- Failed logon attempts allowed: 3
- Reset failed logon attempts after: 30 minutes
- Account will be locked out: Until an administrator manually unlocks the account

3.3. The password requirements for other Trust Staff is:

a) Minimum Password Length: 8

b) Password History: 5

c) Lockout Policy:

- Failed logon attempts allowed: 5
- Reset failed logon attempts after: 20 minutes

- Account will be locked out: For a duration of 20 minutes

3.4. The password requirements for **mainstream students** is:

a) Minimum Password Length: 8

b) Password History: 5

c) Lockout Policy:

- Failed logon attempts allowed: 10
- Reset failed logon attempts after: 10 minutes
- Account will be locked out for: 10 minutes

3.5. There are no minimum password requirements for **special school students**

4. Multi-Factor Authentication (MFA) and Conditional Access:

4.1. Multi-Factor Authentication is enforced for all staff when accessing Microsoft 365 or Remote Access outside of the Trusts network.

4.2. Conditional Access Policies are configured to deny logon attempts for all staff and students from outside the UK.

4.3. If access is to be required outside the UK for a known period, a ticket should be raised on the helpdesk with details, and it will be reviewed and actioned accordingly.

5. Password Expiration:

5.1. We do not enforce password expiration for any accounts. This is now best practice based on UK Gov National Cyber Security Centre (NCSC) guidance. Password policy: updating your approach - NCSC.GOV.UK states:

a) Don't enforce regular password expiry.

b) Regular password changing harms rather than improves security. Many systems will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user and there are costs associated with recovering accounts.

c) Forcing password expiry carries no real benefits because:

- the user is likely to choose new passwords that are only minor variations of the old.
- stolen passwords are generally exploited immediately.
- resetting the password gives you no information about whether a compromise has occurred.
- an attacker with access to the account will probably also receive the request to reset the password.
- if compromised via insecure storage, the attacker will be able to find the new password in the same place.

6. ITS Service & Access Accounts:

6.1. Accounts used for service accounts, or administrative access to applications etc., such as Wireless Controllers, switches, VPN secrets, etc. should all be stored in the ITS BitWarden vault.

6.2. The vault is restricted to ITS engineers and is secured with MFA. Credentials within the vault are structured per school and based on role.

APPENDIX B: Prospere Learning Trust Clear Workspace Protocol

1. **Introduction:**
   1.1. The Trust aims to implement and maintain data protection measures to ensure that personal data is secured away appropriately to assist in the reduction of risk of unauthorised access, loss and damage to information.
   1.2. This protocol is designed to give staff assistance on how to secure personal information (both paper and electronic). This protocol applies to all staff including temporary and agency staff.
   1.3. Staff must abide by the following good practice points when handling personal data.

2. **Leaving a room**
   2.1. Whenever a room is unoccupied for an extended period of time (e.g., overnight / end of working period) you should do the following:
      a) Remove all sensitive and confidential paperwork from plain sight and lock it in a drawer or filing cabinet. This includes mass storage devices such as USB drives and hard drives, or laptops and iPads.
      b) Desks / workspaces should be clear of files / paperwork which may contact data / sensitive information.
      c) Draws should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.
      d) Rooms should be locked.

3. **Confidential waste**
   3.1. All wastepaper which contains sensitive or confidential information must be disposed of either by using the school's onsite secure disposal (shredders) or placed in the designated confidential waste bins.
   3.2. Under no circumstances should this information be placed in regular wastepaper bins.

4. **Computer Screens**
   4.1. Mobile devices, iPads and laptops must be locked away at the end of the day.
   4.2. Computer workstations must be locked when the desk is unoccupied.
   4.3. Computer / laptop screens to be locked when left unattended.

5. **Displays**
   5.1. Passwords should not be left in open areas which are visible to others.
   5.2. Sensitive or confidential personal data should not be left visible or displayed to unauthorised persons.
   5.3. Personal data (including but not limited to seating plans and student lists) shall be stored in folders or in secure places.

6. **Taking data offsite**
   6.1. You are responsible for security of the data in your possession and when transporting it off site you must always take steps to keep it secure.

7. **Printing**
   7.1. Any print jobs containing personal information should be retrieved immediately.

8. **Compliance**
   8.1. If you have misplaced any information, then you must let the Headteacher know as quickly as possible.
   8.2. These guidelines will be monitored for compliance by the School GDPR Lead/School Operations Manager and may include random or scheduled inspections and walkthroughs.